

VERARBEITUNGSSCHUTZ
ZUR VERBESSERUNG DES
DATENSCHUTZES IN
DER MEDIZIN

Konzept und Realisierung

Bernd A. Meyer-Bender

*Ass
München
1986*



Digitized by the Internet Archive
in 2026

Aus dem Rechenzentrum der Ludwig-Maximilians-Universität
München für die Medizinische Fakultät
Vorstand: Prof. Dr. Karl Überla (Vorsitzender)
Leiter: PD Dr. Reinald Greiller

VERARBEITUNGSSCHUTZ ZUR VERBESSERUNG DES
DATENSCHUTZES IN DER MEDIZIN
Konzept und Realisierung

D i s s e r t a t i o n
zum Erwerb des Doktorgrades der Humanbiologie
an der Medizinischen Fakultät der
Ludwig-Maximilians-Universität zu München

vorgelegt von
Bernd A. Meyer-Bender
aus
B o n n
1 9 8 5

Mit Genehmigung der Medizinischen Fakultät
der Universität München

Berichterstatter: Prof. Dr. Karl Überla

Mitberichterstatter: Prof. Dr. Dr. Heinz Goerke
Prof. Dr. Maximilian Knedel

Mitbetreuung durch den
promovierten Mitarbeiter: -

Dekan: Prof. Dr. Wolfgang Spann

Tag der mündlichen Prüfung: 21. Februar 1986

I N H A L T S Ü B E R S I C H T

1.	ZIELE DER ARBEIT	1
2.	HINTERGRUND	4
2.1	Motivation	4
2.1.1	Datenschutz und Datensicherheit als Aufgabe	4
2.1.2	Spezielle Aspekte des Datenschutzes in der Medizin	9
2.2	Gesetzliche Vorschriften	11
2.3	Begriffsbestimmungen	14
2.3.1	Datenschutz und Datensicherheit	14
2.3.2	Gefährdungen	16
2.3.2.1	Zerstörung/Verhinderung	17
2.3.2.2	Datendiebstahl	18
2.3.2.3	Unberechtigte Systembenutzung	19
2.3.2.4	Unberechtigter/unbeabsichtigter Datenzugriff	20
2.3.2.5	Unberechtigte Verarbeitung	21
2.3.3	Gegenüberstellung der Gefährdungen zu den gesetzlichen Vorschriften	23
3.	TECHNISCHE STRATEGIEN UND WERKZEUGE ZUR REALISIERUNG DES DATENSCHUTZES	26
3.1	Grundprinzipien	27
3.2	Ausweisorientierte und listenorientierte Schutzmechanismen	30
3.3	Benutzungsschutz	32
3.4	Kontrollierte Mehrfachverwendung von Daten	36
3.4.1	Grundtechniken	37
3.4.1.1	"Capabilities"	38
3.4.1.2	Zugriffs-Kontrolllisten	41
3.4.2	Zugriffs-Matrix, Objektschutz	44
3.4.3	Vertrauensaspekte	48
3.4.3.1	Informationsschutz	48
3.4.3.2	Funktionale Minimalbefugnisse	53

4.	VERARBEITUNGSSCHUTZ	59
4.1	Bedeutung, Definition	59
4.2	Stand der Technik	60
4.2.1	Teilaspekte in vorhandenen Theorien	60
4.2.2	Die Schlüsselrolle des Programms	62
4.2.2.1	Das Programm als Gefahrenquelle	62
4.2.2.2	Unvollständige Lösungsversuche	63
4.3	Allgemeine Systematik	67
4.3.1	Die dreidimensionale Zugriffs-Matrix	67
4.3.2	Programm-Identifikation und -Authentifikation	70
4.4	Realisierung	72
4.4.1	Rahmenbedingungen	72
4.4.1.1	Betriebssystem	72
4.4.1.2	Das Prinzip der unbekannten Datei-Kennwörter	74
4.4.2	Methodik	76
4.4.3	Projektstand	79
4.4.4	Abschätzung des Sicherheitsgewinns	81
4.4.4.1	Praktische Erfahrungen	81
4.4.4.2	Sicherheit des Monitors	82
4.4.4.3	Grundsätzliche Schwachstellen, Ausblicke	84
4.5	Systemverwalter, Datenschutzbeauftragter	86
5.	ZUSAMMENFASSUNG	89
6.	SCHRIFTTUMSVERZEICHNIS	94

DANK

Mein aufrichtiger Dank gilt Herrn Professor Dr. Karl Überla, der keine Zeit und Mühe gescheut hat, mich zu beraten, und der sich intensiv mit der vorliegenden Arbeit befaßt hat. Ebenso danke ich meinem Freund, Herrn Dr. Richard Schrag, der mir stets als Gesprächspartner zur Verfügung stand, und der somit wesentlich dazu beigetragen hat, daß mancher Gedanke reifen konnte. Auch meinem überaus großzügigen Vorgesetzten, Herrn PD Dr. Reinald Greiller, und meinem Freund, Herrn Dr. Herbert Seidel, bin ich für ihre Ermunterung und ihre guten Ratschläge zu großem Dank verpflichtet.

Zuletzt, aber in besonderem Maße, danke ich meiner Familie, die mit großer Geduld auf manche Stunde mit mir verzichtete, allem voran meiner Frau, Gerlinde, die zudem die mühsame Arbeit übernahm, all die vielen Schreibfehler im Manuskript aufzuspüren. Ich hoffe zuversichtlich, daß das vollendete Werk eine gewisse Entschädigung für sie darstellt.

1. ZIELE DER ARBEIT

Die vorliegende Arbeit befaßt sich vorrangig mit technischen Methoden, die geeignet sind, Datenschutz und Datensicherheit in Datenverarbeitungsanlagen zu gewährleisten. Dabei werden drei Hauptziele verfolgt:

- i) die wichtigsten, bisher veröffentlichten Strategien zur technischen Verwirklichung von Datenschutz und Datensicherheit zusammenzustellen (Abschnitt 3);
- ii) aufzuzeigen, daß es einen zentralen Aspekt gibt, den diese bisher bekanntgewordenen, technischen Schutzmechanismen nicht abdecken, und eine erweiterte Systematik vorzustellen, die diese Lücke ausfüllt (Abschnitte 4.1 - 4.3);
- iii) eine praktisch erprobte Realisierung des neu entwickelten Prinzips zu beschreiben und kritisch zu bewerten (Abschnitte 4.4, 4.5).

Das neue Verfahren soll, ebenso wie die zugrundeliegende, weiterführende Theorie mit dem Begriff "Verarbeitungsschutz" bezeichnet werden.

Trotz der damit definierten streng technischen Thematik muß der Hintergrund, der Schutzmaßnahmen erst erforderlich macht, als Ausgangspunkt genommen werden - nicht zuletzt, um den hohen Stellenwert des Verarbeitungsschutzes zu belegen (Abschnitt 2). Daß eine einseitige Sicht der Datenschutzproblematik Gefahren birgt, konstatieren bereits Saltzer und Schroeder [61], die eine gegenseitige Ergänzung der sozialpolitischen und technischen Aspekte fordern; denn bei einer zu engen Betrachtungsweise wird das Gefahrenbewußtsein auf den betrachteten Sektor beschränkt und damit ein falsches Vertrauen geweckt. Um adäquat, d.h. im richtigen Wirkungsbereich, auf mögliche Gefahren reagieren zu können, ist ein vollständiges Bild der Gefahrenquellen anzustreben. Zu einer umfassenden Behandlung des Gesamtthemas Datenschutz und Datensicherheit gehören u.a.:

- humanitäre, soziologische und politische Aspekte,
- juristische Forderungen und Implikationen;
- spezielle Bedürfnisse einzelner Fachbereiche (z.B. Medizin²),
- bauliche, organisatorische und personalpolitische Maßnahmen³ sowie
- der Entwurf von sicheren Hard- und Software- Architekturen.

Eine umfassende Darstellung dieser Komplexe geben u.a. Hoffmann [31] und Martin [46].

¹ Gallwas et al. [19], Mallmann [45], Sieber [67] u.a.m.

² Barber et al. [2], Griesser [26], Griesser et al. [28], Kilian et al. [35], Reichertz, Kilian [57] u.a.m.

³ Bates [3], Graham, Denning [22], Kilian et al. [35], Lindemann et al. [43], Palme [49], Stadler [71], Turn, Ware [76] u.a.m.

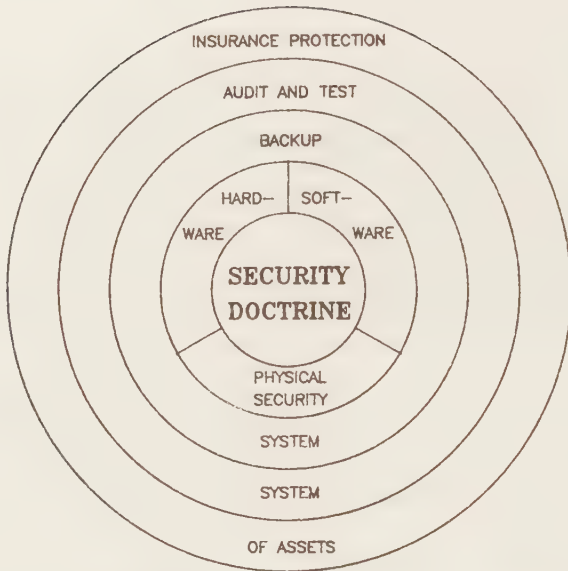


Abb 1: Aufbau eines Datenschutz-Systems nach Bates

Die Eingrenzung des zentralen Themas dieser Arbeit auf technische Fragen ist jedoch nicht schädlich, wenn dies auf der Grundlage des Gesamthintergrundes geschieht. Bates [3] legt dar, daß es zur Verwirklichung der Datensicherheit einer im voraus festzulegenden Sicherheits-Strategie ("security doctrine") bedarf. Von dieser Basis ausgehend sind dann die erforderlichen Maßnahmenkomplexe zu verwirklichen, wobei eine schalenartige Struktur entsteht (Abb. 1). Obwohl Bates offensichtlich eine sehr globale Betrachtungsweise ansetzt (bis hin zur Versicherung für den Schadensfall), ist doch auffallend, daß die innerste Schale ausschließlich technische Maßnahmen enthält; sie bilden die unverzichtbare erste Schutzschicht. Man muß folglich davor warnen, sich etwa übermäßig auf organisatorische Maßnahmen zu verlassen; denn mit ihrer Perfektionierung wächst ihre Komplexität⁴ und damit auch die Gefahr, daß sie aus rein menschlichen Motiven (oder Unzulänglichkeiten) heraus unterlaufen werden. Der Verfasser ist der Meinung, daß jede (sinnvolle) technische erzwungene Maßnahme, durch die sich eine organisatorische Vorschrift erübrigt, als Sicherheitsgewinn zu bezeichnen ist. Daß dies nicht immer möglich ist, zeigt allerdings Abschnitt 2.3.2 (z.B. bei Zerstörung/Verhinderung

⁴ S. z.B. Stadler [71].

und bei Datendiebstahl).

Wenn also in dieser Arbeit von Abschnitt 3 an fast ausschließlich technische Gesichtspunkte zur Sprache kommen, so ist dies mit der aufgezeigten Kernfunktion als zentrale Schuttschicht begründet. Die Berechtigung hierzu läßt sich auch aus der von Schulze [66] festgestellten Tatsache ableiten, daß "sich die in der elektronischen Datenverarbeitung erforderlichen Schutzmaßnahmen nicht grundsätzlich, sondern nur dem Grade nach von denjenigen unterscheiden, die bei anderen Formen der Datenverarbeitung angemessen sind. Neu ist allerdings, daß das Werkzeug der Datenverarbeitung (der Computer) eine entscheidende Rolle bei der *Gefahrenabwehr* spielt".

Im folgenden Abschnitt 2 soll der allgemeine Hintergrund deshalb nur insofern beleuchtet werden, als nötig ist, um

- eine kurze Begründung für den Datenschutz und die Datensicherung im allgemeinen und speziell auf die Medizin bezogen zu geben,
- den gesetzlichen Rahmen abzustecken, der die Verpflichtung zum Datenschutz im personenbezogenen Bereich präzisiert, und
- eine Einteilung der Gefährdungen für Datenschutz und Datensicherheit anzugeben, die eine Einordnung der technischen Maßnahmen erleichtert.

2. HINTERGRUND

2.1 Motivation

2.1.1 Datenschutz und Datensicherheit als Aufgabe

Seit der Mitte der 60-er Jahre, als der breite Einsatz der elektronischen Datenverarbeitung (EDV) allmählich verwirklicht wurde, spielen die Begriffe "Datensicherheit" und "Datenschutz" in den Überlegungen der Verantwortlichen und Betroffenen eine zunehmende Rolle. Die inzwischen entstandene Abhängigkeit weiter Teile der Gesellschaft von der EDV ist eine Tatsache, die nicht geleugnet werden kann.⁵ Diese Abhängigkeit betrifft zum einen

- die Verfügbarkeit und Korrektheit von Daten sowie
- die Funktionsfähigkeit und Zuverlässigkeit der Apparaturen und Programme, mit denen sie im weitesten Sinne verarbeitet werden.

Zum anderen aber besteht die dringende Notwendigkeit, das Recht auf den Zugriff zu bestimmten Daten bzw. auf deren Verarbeitung einzuschränken. Diese beiden Aspekte können nicht unabhängig voneinander betrachtet werden; denn die Korrektheit der Daten ist beispielsweise gefährdet, wenn beliebige Personen befähigt sind, sie zu verändern.⁶

Vom Betroffenen aus gesehen, lassen sich mindestens drei Motivkreise unterscheiden, die hinter der Forderung stehen, den Zugriff auf Daten einzuschränken:

- staatliche, speziell militärische Geheimhaltung,
- kommerzielle Interessen und
- Persönlichkeits-Schutz.

Die Gründe für militärische Geheimhaltung und dergleichen liegen auf der Hand; die Schwierigkeit einer näheren Analyse ist aus der Sache verständlich. Es ist wohl kein Zufall, daß große Teile der Erkenntnisse auf dem Gebiet des Datenschutzes im militärischen Umfeld entwickelt wurden, und es muß damit gerechnet werden, daß manche methodischen Erkenntnisse noch heute der Geheimhaltung unterliegen.

Der kommerzielle Datenschutz richtet sich zunächst gegen die Preisgabe von technischen und ökonomischen Betriebsgeheimnissen, sowie gegen Unterschlagung, Betrug o.ä. durch eigene Mitarbeiter, Geschäftspartner oder Dritte. Der Bruch dieser Schutzbedürfnisse wird landläufig als "Computer-

⁵ Für Beispiele s. Martin [46].

⁶ Linden [44] zeigt, daß Sicherheits- und Zuverlässigkeitsfragen oft mit den gleichen Mitteln behandelt und gelöst werden können und müssen.

Kriminalität"⁷ bezeichnet. Hinzu kommen aber meist auch innerbetriebliche Notwendigkeiten; unter anderem

- ist die hierarchische Struktur einer Organisation mit den entsprechenden Befugnissen abzubilden,
- sind die Informationen unabhängiger Abteilungen (Personal, Entwicklung, Vertrieb, Buchführung usw.) je vertraulich zu behandeln,
- muß das "Vier-Augen-Prinzip" bei wichtigen Eingriffen in die gespeicherte Information erzwingbar sein.

Die militärischen und kommerziellen Schutzbedürfnisse sind von der Motivation her unproblematisch, da aus der Sicht des "Besitzers" kein Konflikt zum Verarbeitungsziel besteht, d.h. der Inhaber der Daten ist auch daran interessiert, sie zu schützen. Die Daten betreffen "Objekte", die zum selben Verfügungskreis gehören⁸.

Anders verhält es sich beim Schutz der Daten menschlicher Individuen - offensichtlich, weil die "Objekte", die durch die Daten beschrieben werden, und die wohl in einem gewissen Sinn deren "Eigentümer" sind, gerade *nicht* dem "Besitzer" der Daten "verfügbar" sein dürfen. Das soll natürlich nicht heißen, daß der Besitz und die Verarbeitung von persönlichen Daten stets gegen die Interessen des Individuums verstoßen; Thomas J. Watson Jr. hat 1968 in einer Rede⁹ eine Vielzahl von Fällen aufgezählt, in denen die Allgemeinheit oder einzelne Individuen von einer gewissen Datenverfügbarkeit profitieren. Manche seiner allzu fraglos vorgestellten Beispiele zeigen aber aus heutiger Sicht sehr deutlich, daß es schwierige Grenzbereiche gibt, in denen Konflikte entstehen zwischen Allgemeinwohl (z.B. Kriminalitätsbekämpfung) und Privatsphäre¹⁰ aller Bürger, funk-

⁷ Für Beispiele s. Bates [3], Martin [46], Sieber [67], Turn und Ware [76] u.a.m. Eine im allgemeinen weniger verbrecherische Abart ist das derzeit beliebte Hobby des "hacking", dessen Anhänger Freude daran haben, mit Hilfe von Kleincomputern unter Umgehung von Schutzvorkehrungen in Großsysteme "einzubrechen". Dieser Zeitvertreib kann durchaus positive Folgen haben, wenn er auf Sicherheitsmängel hinweist, die zu beseitigen sind. Allerdings trägt er auch zu der noch darzustellenden Verunsicherung der Allgemeinheit der Datenverarbeitung gegenüber bei.

⁸ Es darf allerdings nicht übersehen werden, daß in neuester Zeit Forderungen von außen an die Besitzer von Daten herangetragen werden, die Geheimhaltung gezielt zu lockern, etwa wenn es darum geht, die mehrfache Durchführung von Tierversuchen überflüssig zu machen, oder die Ursachen von Umweltschäden aufzuspüren.

⁹ Zitiert von Martin [46], Kapitel 4.

¹⁰ Es sprengt den Rahmen dieser Arbeit, auf die umstrittene Definition des Begriffs "Privatsphäre" einzugehen; da es zweifelsfrei ein derartiges, zu schützendes Gut gibt, wird das Wort hier ganz naiv benutzt; zu dieser juristisch grundsätzlichen Frage s. Steinmüller [72], [73].

tionsgerechter Verwaltung und Bürokratie, demokratischem Auftrag und Minderheitenschutz usw.

Setzt man aber voraus, daß die Speicherung und Verarbeitung einer gewissen Datenmenge aus ethischer und demokratischer Sicht vertretbar oder gar erwünscht ist, besteht meist immer noch die ernste Befürchtung, daß der berechnete Besitzer der Daten sie über die zulässige Aufgabe hinaus zu anderen Zwecken mißbrauchen oder weiterleiten könnte. Im letzten Fall ist damit zu rechnen, daß eine Proliferation personenbezogener Daten - und besonders deren Zusammenführung aus unterschiedlichen Quellen - eine praktisch unbegrenzte Auswertung¹¹ ermöglicht, die sich jeder Kontrolle entzieht.

Der Ruf nach Persönlichkeitsschutz gründet also in der Erkenntnis, daß der Zugriff auf Daten, die zur Privatsphäre eines Menschen gehören, durch Instanzen, die diese Daten nicht (nur) für eine Tätigkeit zugunsten des Betroffenen benötigen, diesen in seinen bürgerlichen Freiheiten einschränken und ihm auch sonst erheblichen Schaden zufügen kann. Diese Feststellung ist beim Bruch des ärztlichen Geheimnisses¹² oder beim Bekanntwerden des finanziellen Status eines Menschen evident!¹³ Es sind aber auch Situationen denkbar, in denen der Zugriff auf wesentlich weniger sensitiv erscheinende Daten wie Hobbys, Religion oder Verhalten als Autofahrer in globaler Sicht schädlicher als im Rahmen einer begrenzten Aufgabe sein kann.

Neben diesen offenkundigen Gründen für den Datenschutz darf ein sozialpolitischer Aspekt nicht übersehen werden. Bereits 1967 erklärte der US-amerikanische Senator Sam J. Ervin Jr., daß der Computer zum Bösewicht der Gesellschaft gestempelt würde, wenn man die - damals noch - verbleibende Zeit nicht nutze, um ethische Maßstäbe zu entwickeln und durchzusetzen!¹⁴ Eines der ersten Menetekel für das Eintreten der vorhergesagten Tendenz ist in dem Lied "Three-Five-Zero-Zero" aus dem Musical "Hair" zu finden (auch wenn es sich äußerlich eher auf den Vietnam-Krieg als auf den Persönlichkeitsschutz bezieht), in dem die elektronische

¹¹ In jüngster Zeit wird oft das Schlagwort vom "gläsernen Menschen" verwendet, um den Zustand der totalen und zentralen datenmäßigen Erfassung auszudrücken.

¹² S. z.B. Griesser et al. [28], Abschnitt 1.0

¹³ Dem Verfasser sind Fälle von Banken bekannt, die in Großbetrieben eingerichtete Filialen wieder aufgaben, weil sie dort kaum Kreditgeschäfte tätigen konnten wegen der Sorge, Kollegen oder die Personalabteilung könnten davon erfahren; die berühmt/berühmten "Nummernkonten in der Schweiz" bekunden die gegenteilige Vorsicht.

¹⁴ Hoffmann [32] zitiert aus der Rede vom 1. Mai 1967: "If self-regulation and self-restraint are not exercised by all concerned with automatic data processing, public concern will soon reach a stage where strict legislative controls will be enacted, government appropriations for research and development will be denied. The computer will become the villain of our society."

Datenverarbeitung unmittelbar in eine Horrorvision der Unmenschlichkeit einbezogen wird. Vorläufiger Höhepunkt dieser Entwicklung sind in der Bundesrepublik Deutschland die Diskussionen über das Volkszählungsgesetz 1983¹⁵ und über die Gesetzesinitiative zur Einführung eines maschinenlesbaren Personalausweises, in die sich neben sachlich unanfechtbaren Vorbehalten und Sorgen auch emotionsgeladene Obstruktionsaufrufe mengten!¹⁶ Von Senator Ervins Rede führt offensichtlich eine gerade Linie zur Negation (mindestens) der personenbezogenen Datenverarbeitung schlechthin; und dies, obwohl die in derselben Rede vorhergesehene, strenge Gesetzgebung verwirklicht wurde, ja in der Bundesrepublik Deutschland zu den anspruchvollsten der Welt gezählt werden darf!¹⁷

Es kann kaum verwundern, daß es auch gewichtige Gegnerschaft gegen den Datenschutz bzw. dessen strenge Auslegung gibt. Als erstes sind natürlich die Instanzen und Institutionen zu nennen, die vom freien Datengebrauch "profitieren"; und hier ist in erster Linie der "Staat" angesprochen. In einer totalitären Umwelt hat Datenschutz im personenbezogenen Bereich keinen oder keinen hohen Stellenwert. In demokratischen Gemeinwesen westlicher Prägung dagegen ist es eine nicht nur beim Einsatz der DV¹⁸ gestellte, stets neue Aufgabe, die Interessen des Einzelnen und die der Allgemeinheit gegeneinander auszubalancieren; daher dürfte der Persönlichkeitsschutz als solcher weniger umstritten sein, als vielmehr die Grenzziehung zwischen vertretbarer und unstatthafter Verwendung der Daten. Diese Grenzziehung ist sicherlich mit dem weltanschaulichen Standpunkt der jeweiligen Betrachter korreliert; doch darf nicht übersehen werden, daß jede Regierung - gleich welcher Couleur -

- die Neigung hat, die eigene politische Ansicht mit dem Gemeinwohl gleichzusetzen und
- zunächst motiviert ist, alle Mittel, die zum Erreichen der politischen Ziele verfügbar sind - und dazu gehört neuerdings zweifellos die EDV - auch auszunutzen.

¹⁵ Das Gesetz wurde zwar durch ein Urteil des Bundesverfassungsgerichts für ungültig erklärt; die Auseinandersetzung wird aber bei einer neuerlichen Gesetzesinitiative zweifellos wieder aufflammen.

¹⁶ Es ist wohl nicht nur eine Pikanterie, daß ein Teil dieser Gegnerschaft in den gleichen Reihen zu finden ist, welche die in Fußnote 8 erwähnte, teilweise Aufhebung des Datengeheimnisses fordern; vielmehr dürfte es ein Symptom dafür sein, daß die sozialpolitischen Qualitätsunterschiede in der Datenverarbeitung noch nicht in ausreichendem Maße analysiert und berücksichtigt wurden.

¹⁷ S. Abschnitt 2.2; das Bundesdatenschutzgesetz (BDSG) ist allerdings auch keineswegs unumstritten - s. hierzu Gallwas et al. [19], Einleitung, Abschnitt 7.1

¹⁸ Die EDV unterscheidet sich nicht prinzipiell von anderen informationsverarbeitenden Verfahren, sondern nur in der Leistungsfähigkeit; Steinmüller [72]: "Verwaltung ist Datenverarbeitung".

Eine weitere Kritikergemeinde ist dem Datenschutz unter den Datenverarbeitern, den Fachleuten, erwachsen. Sie fühlen sich oft durch die Schutzmaßnahmen in ihrer Arbeit behindert. Dies kann natürlich auf einen Mangel an Einsicht in die Implikationen und Folgen der eigenen Tätigkeit liegen; weit häufiger dürfte jedoch gelten, daß die Arbeit mit *nicht* schutzwürdigen Daten (und das ist sicherlich die große Mehrzahl) durch allzu globale Schutzmaßnahmen unsachgerecht erschwert wird. In diesem Zusammenhang ist es interessant, daß Stirling [74] einen potentiellen Gegensatz zwischen dem Persönlichkeitsschutz und der Humanisierung des Umgangs mit DV-unterstützten Informationssystemen erkennt. Es scheint dringend geboten, diesen Widerstand der Fachleute abzubauen; denn sie haben es schließlich in der Hand, mögliche Sicherheitsmaßnahmen anzuwenden oder zu umgehen.

In manchen Fällen kann auch die *Nicht-Weitergabe* von Informationen für die Person, die sie beschreiben, nachteilige Auswirkungen haben und somit einen - berechtigten - Widerstand gegen allgemein gültige Datenschutzmaßnahmen begründen. So meldet Greiser [24], daß "die epidemiologische und sozialmedizinische Forschung durch Gesetze und Vorschriften, die den Zugang zu personenbezogenen Daten regeln, gegenwärtig (Anm. d. Verf.: 1979) schwer beeinträchtigt und zum Teil zum Erliegen gekommen" ist, und führt zahlreiche Beispiele für Ergebnisse auf, die nach damals geltender Rechtslage nicht mehr erzielbar gewesen wären!¹⁹ Diese scheinbare Übervorsicht des Gesetzgebers beruht offensichtlich auf zwei Befürchtungen:

- wenn erst ein Mechanismus geschaffen ist, um Daten an zentralen Einrichtungen sinnvoll und berechtigt zusammenzuführen, könnte er - wie bereits erwähnt - auch ausgenutzt werden, um andere, schädliche Auswertungen durchzuführen;
- auch wenn der "Eigentümer" von Daten deren Weitergabe an explizit aufgezählte Dritte zustimmt, entgleiten sie damit leicht der Kontrolle; es besteht die Gefahr, daß
 - eine sekundäre Weitergabe nicht bemerkt wird oder nicht verhindert werden kann, und dadurch unkontrollierte, weitergehende Datensammlungen kompiliert werden können;²⁰
 - ein vom Gesetzgeber vorgesehenes, nachträgliches Korrektur-, Sperr- oder Löschverlangen bzw. der Widerruf der Speichererlaubnis nur unvollständig wirksam wird.

Es wird noch in Abschnitt 3.4.1.1 zu zeigen sein, daß diese Sorgen elementaren Gefährdungen entsprechen, denen jede Mehrfachverwendung von Daten ausgesetzt ist.

¹⁹ S. hierzu auch Wagner [77] sowie [85].

²⁰ S. z.B. Lenk [42].

Die Einwände gegen den Datenschutz müssen unbedingt ernstgenommen werden; denn es ist schier unmöglich, Maßnahmen durchzusetzen, gegen die massive Ablehnung besteht. Diese Frage kann aber im Rahmen dieser Arbeit nur indirekt (d.h. im Sinne, daß Methoden bevorzugt werden, die den aufgezeigten, psychologischen Schranken entgegenwirken) verfolgt werden, da sie schwerpunktmäßig auf die bislang oft unbefriedigende *Durchsetzung* des Datenschutzes ausgerichtet ist. Nur die Fähigkeit, Datenschutz zu erzwingen;²¹ kann Grundlage für Überlegungen sein, unter welchen Umständen es ethisch statthaft oder geboten ist, einen kontrollierten Datenaustausch oder dergleichen zu gestatten.

Soll die personenbezogene Datenverarbeitung auch weiterhin die Aufgaben erfüllen, die sie zweifellos zum Wohl der Menschheit zu leisten vermag, so muß sie von dem Odium der unabsehbaren Gefährdung für ihn befreit werden, in das sie - gewiß nicht gänzlich zu unrecht - bei einem großen Teil der Bevölkerung geraten ist. Dies kann nach Auffassung des Verfassers nicht gelingen, wenn sich die mit dem Datenschutz beauftragten Instanzen damit begnügen (müssen), organisatorische Maßnahmen zu verordnen und - so gut es geht - zu überwachen; denn gerade den mit der Organisation und Abwicklung des Schutzes Betrauten gilt das öffentliche Mißtrauen (meist zu unrecht). Ziel muß es deshalb sein, die *technischen* Möglichkeiten auszubauen und auszuschöpfen, die eine Verletzung des Datenschutzes möglichst zuverlässig ohne menschliches Zutun verhindern sollen.²² Aber auch wenn eine solche zuverlässige, technische Sicherung der Daten vor Mißbrauch gelingt, wird noch eine umfangreiche Öffentlichkeitsarbeit erforderlich sein, um das Endziel, das Vertrauen der Bevölkerung, zu erreichen.

2.1.2 Spezielle Aspekte des Datenschutzes in der Medizin

Schon lange bevor es den Begriff Datenschutz oder gar Datenverarbeitung gab, hat es im medizinischen Sektor ein waches Bewußtsein für den Persönlichkeitsschutz gegeben. Die ärztliche Schweigepflicht dürfte eine der ältesten, allgemeinen Vertraulichkeitsverpflichtungen sein. Deshalb ist es kaum verwunderlich, daß der Datenschutz gerade in der Medizin starke Beachtung fand, sobald die Datenverarbeitung auch in diesem Fachgebiet eingesetzt wurde. Der Arzt selbst ist außerordentlich daran interessiert, Vertraulichkeit zu wahren, da dies eine unverzichtbare Basis für das heilungs-

²¹ S. den Begriff der Abschottung in Abschnitt 3.4; auch hier ist die Lockerung einer zunächst total undurchlässigen Trennschicht die sicherste Methode, *kontrollierten* Datenaustausch zu ermöglichen.

²² Dieses Ziel müßte ganz im Sinne der Datenschutzinstanzen sein; denn es würde ihre Arbeit wesentlich erleichtern, vor allem aber ihnen selbst Rückhalt geben und ihnen erlauben, sich verstärkt auf die verbleibenden, unumgänglich organisatorisch zu lösenden Probleme zu konzentrieren.

notwendige Vertrauensverhältnis zum Patienten ist. Das selbstverständliche Verhältnis der Ärzte zur Vertraulichkeit ehrt diese zwar, führt aber andererseits oft zu einem unterentwickelten Problembewußtsein. Denn die Gefahr geht nicht von diesem Personenkreis aus, sondern von denjenigen, die ebenfalls zu den einmal maschinell erfaßten Daten zugreifen können, aber weder die gleiche Motivation haben, noch in vielen Fällen die Sachkenntnis zu ihrer richtigen Deutung²³. Die Verpflichtung von Verwaltungspersonal, DV-Spezialisten usw. auf die ärztliche Schweigepflicht und auf den Datenschutz kann zwar das ethische Bewußtsein stärken, ist aber nicht mit dem Eigeninteresse des Arztes an der Schweigepflicht vergleichbar.

Der Bruch des ärztlichen Geheimnisses kann aber sowohl was Massendaten betrifft, als auch in Bezug auf Individuen, "Außenstehern" wie Versicherungen, Werbeagenturen, sensationsorientierten Massenmedien oder Arbeitgebern erheblichen Gewinn versprechen. Zwar ist es oft leichter, mit einem weißen Kittel bekleidet, konventionell gespeicherte Daten - Karteikarten oder dergleichen - zu entwenden oder einzusehen, doch ist es ein allgemein einsetzbarer Vorteil der Datenverarbeitung, daß eine einmal entwickelte Methodik wiederholt und auf beliebige Datenmengen gleicher Struktur anwendbar ist.

Größere Probleme können auch im Zuge der derzeit fortschreitenden Dezentralisierung von DV-Leistungen auftreten; wenn etwa Medikamentenanforderungen oder Diagnoseauskünfte auf Station "per Knopfdruck" erreichbar sind, könnten z.B. süchtige Pfleger oder mißtrauische, DV-geübte Patienten - vor allem bei schwach besetzten Nacht- oder Wochenendschichten - leicht auf den Gedanken kommen, die vorhandenen Geräte auszunutzen, wenn kein Riegel vorgeschoben wird.

Die aufgezählten Probleme findet man in leicht unterschiedlichen Ausprägungen allenthalben, wenn es darum geht, Daten vor Mißbrauch zu schützen; sie werden nur im medizinischen Bereich durch die Unmittelbarkeit des persönlichen Bezugs und die lange Tradition des Vertrauens verstärkt wahrgenommen. So spielt das Thema Datenschutz in der Medizin eine Rolle als Spezialdisziplin in der allgemeinen Problemstellung, auch wenn dies weniger technisch als menschlich zu verstehen ist. Dementsprechend gibt es eine relativ umfangreiche Spezialliteratur zu diesem Thema, die von rechtlichen Aspekten²⁴ über grundsätzliche Gesichtspunkte²⁵ bis zu praktischen, medizinbezogenen Lösungswegen²⁶ reicht.

²³ Auf die Kontextabhängigkeit medizinischer Daten weist Reichertz [58] hin; Rienhoff [59] macht auf die Problematik des Richtigkeitsbegriffs bei solchen Informationen aufmerksam.

²⁴ Kilian, Porth [36].

²⁵ Z.B. Barber et al. [2], Greiller, Überla [23], Griesser [26] und Reichertz, Kilian [57].

²⁶ Z.B. Griesser et al [28].

Eine gewisse Sonderstellung nehmen epidemiologische Untersuchungen, medizinisch-statistische "Querschnittsuntersuchungen" und dergleichen ein, bei denen "anonymisierte" Daten verwendet werden. Für die Krankenversicherungsträger sind die Grundlagen und Einschränkungen in §369 Abs. 2 Reichsversicherungsordnung (RVO) festgehalten. Hier, wie bei der wissenschaftlichen Verwendung, wird davon ausgegangen, daß solche Daten nicht mehr empfindlich im Sinne des Persönlichkeitsschutzes sind. Obwohl es zunächst plausibel erscheint, die Ausbreitung solcher Daten nicht durch Schutzmaßnahmen einzuschränken, muß festgestellt werden, daß es erwiesenermaßen fast durchweg möglich (und für die Auswertung solcher mit anonymisierten Daten gewonnenen Ergebnisse sogar erforderlich) ist, die Anonymität wieder rückgängig zu machen, sofern sie in einer Form vorliegen, die noch subjektbezogen ist, die individuellen Bezüge also noch nicht durch statistische Verarbeitung verdeckt worden sind. Auch wenn eine Rücktransformation nicht a priori vorgesehen ist, kann oft geschicktes Fragen ausreichen, um die Anonymität zu durchbrechen.²⁷ Fatalerweise ist dies um so leichter, je seltener - und somit sensibler - die gespeicherten Informationen sind. Schutzmaßnahmen gegen solche "Entanonymisierung" sind äußerst komplex²⁸ und verstoßen zudem meist gegen die oben geforderte Humanisierung des Umgangs mit DV-unterstützten Informationssystemen.

Der "Datenschützer" neigt leicht dazu, nur noch die Möglichkeiten zum Bruch der Vertraulichkeit zu sehen. In der Tat ist der Verfasser jedoch der Ansicht, daß die Datenschutzdziplin gerade in der Medizin erfreulich ist, und diese Ansicht wird durch eine vieljährige Erfahrung getragen. Doch dies entpflichtet nicht, es dem denkbaren "Spion" möglichst schwer zu machen. Nicht zuletzt gilt es auch hier, Mißtrauen in der Öffentlichkeit abzubauen;²⁹ um das für die Heilung erforderliche Vertrauensverhältnis nicht zu gefährden. Dies gilt in besonderem Maß in großen Universitätskliniken, in denen der Patient selten lange und ausschließlich von einem Arzt betreut wird.

2.2 Gesetzliche Vorschriften

Der Datenschutz ist im kommerziellen und militärischen Bereich im Interesse des Betreibers der EDV; man kann es deshalb diesem überlassen, geeignete Maßnahmen zu dessen Verwirklichung zu ergreifen. Dasselbe gilt in allen Berei-

²⁷ Denning et al. [10], Palme [49], Saltzer, Schroeder [62], Schlörner [63] u.a.m.

²⁸ Dobkin et al. [16].

²⁹ Wie stark dieses Mißtrauen ist, erfuhr der Verfasser vor einiger Zeit, als er sich bei einer Bekannten, von deren Kaiserschnitt er über gemeinsame Freunde erfahren hatte, nach ihrem Befinden erkundigte, und daraufhin von dieser massiv beschuldigt wurde, den Datenschutz verletzt zu haben - dabei war es ihm gar nicht bekannt, daß der Eingriff in dem Klinikum durchgeführt worden war, in dem er beschäftigt ist!

chen bezüglich der allgemeineren Erfordernisse der Datensicherung. Was den Persönlichkeitsschutz angeht, von dem in den letzten Abschnitten gezeigt wurde, daß die betroffene Person keinen unmittelbaren Einfluß auf den Gebrauch der zugeordneten Daten hat, hat sich der Gesetzgeber veranlaßt gesehen, bürgerfreundliche Normen zu erlassen, sowohl gegen die nicht-staatliche Benachteiligung oder Manipulation des einzelnen, als auch gegen eine übermächtige Verletzung der Privatsphäre durch staatliche Organe.

In der Bundesrepublik Deutschland ist bereits die wesentliche Aussage im Grundgesetz enthalten: die Art. 1, Abs. 1 und Art. 2, Abs. 1 bieten eine Handhabe im Sinne der Grundrechte.³⁰ Aber auch in Einzelgesetzen finden sich einschlägige Bestimmungen. So sind z.B. im Fernmeldegesetz (§§ 10, 11) und in der Abgabenordnung (§30) Geheimhaltungsvorschriften zugunsten der betroffenen Personen erlassen. §369, Abs. 2 der Reichsversicherungsordnung (RVO) schreibt die Anonymisierung von Daten vor, die zur Früherkennung von Epidemien usw. dienen, und §203 des Strafgesetzbuchs regelt die strafrechtliche Seite der Verletzung von Privatgeheimnissen.³¹

Speziell auf die EDV bezogen - und auf die Erfahrung mit bereits vorher erlassenen Gesetzen in den Ländern Hessen und Rheinland-Pfalz zurückgreifend - hat der Bundestag 1977 das Bundesdatenschutzgesetz (BDSG) in Kraft gesetzt. Inzwischen haben alle anderen Länderparlamente ebenfalls Datenschutzgesetze verabschiedet, die sich im wesentlichen nur insofern vom BDSG unterscheiden, als sie auf die Kompetenzbereiche der Länder bezogen sind, und gelegentlich länderspezifische Besonderheiten Eingang gefunden haben. Von Bedeutung für die vorliegende Arbeit ist die Tatsache, daß alle Ländergesetze eine Anlage (bzw. im Fall des BayDSG einen Artikel) enthalten, die der "Anlage zu §6 Abs. 1, Satz 1" des BDSG entspricht. Die darin enthaltenen "Zehn Gebote des Datenschutzes" schreiben vor, daß spezielle Kontrollmaßnahmen durchzuführen sind; wörtlich heißt es:

"Werden personenbezogene Daten automatisch verarbeitet, sind zur Ausführung der Vorschriften dieses Gesetzes Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

- 1.) Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (*Zugangskontrolle*),
- 2.) Personen, die bei der Verarbeitung personenbezogener Daten tätig sind, daran zu hindern, daß sie Datenträger unbefugt entfernen (*Abgangskontrolle*),
- 3.) die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung

³⁰ Es ist interessant zu vermerken, daß die (ältere) Verfassung der Vereinigten Staaten von Amerika a priori keine entsprechenden Bestimmungen enthielt, und deswegen ergänzt werden mußte; s. Hoffman [32].

³¹ Für weitergehende Angaben s. Gallwas et al. [19] Einleitung, Abschnitt 1.3.

- gespeicherter personenbezogener Daten zu verhindern (*Speicherkontrolle*),
- 4.) die Benutzung von Datenverarbeitungssystemen, aus denen oder in die personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden, durch unbefugte Personen zu verhindern (*Benutzerkontrolle*),
 - 5.) zu gewährleisten, daß die zur Benutzung des Datenverarbeitungssystems Berechtigten durch selbsttätige Einrichtungen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (*Zugriffskontrolle*),
 - 6.) zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden können (*Übermittlungskontrolle*),
 - 7.) zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (*Eingabekontrolle*),
 - 8.) zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (*Auftragskontrolle*),
 - 9.) zu gewährleisten, daß bei der Übermittlung personenbezogener Daten sowie beim Transport entsprechender Datenträger diese nicht unbefugt gelesen, verändert oder gelöscht werden können (*Transportkontrolle*),
 - 10.) die innerbehördliche und innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (*Organisationskontrolle*).

Man erkennt leicht, daß diese Forderungen teilweise unterschiedliche Qualität haben³² und daß sie nicht frei von gelegentlich verwirrenden Überschneidungen³³ sind; bemerkenswerterweise wird nicht gefordert, lesende Zugriffe auf personenbezogene Daten zu protokollieren. Dennoch müssen sich in der Bundesrepublik Deutschland alle Maßnahmen zum Persönlichkeitsschutz - bzw. deren Mängel - an diesen Normen messen lassen.³⁴

³² Zum einen geht es darum, unbefugte Benutzung zu verhindern, zum anderen sollen Überprüfungsmöglichkeiten gewährleistet werden usw.

³³ So kann beispielsweise die Benutzerkontrolle bei restriktiver Auslegung des Begriffs der automatischen Übermittlung eine zwingende Voraussetzung für die Speicherkontrolle sein, geht aber über deren Forderungen hinaus, indem sie nicht nur auf die Kennungen mit personenbezogenen Daten bezogen wird, sondern auf das Gesamtsystem, sofern überhaupt personenbezogene Daten gespeichert sind.

³⁴ S. auch Gallwas et al. [19], Kommentar zur Anlage zu §6 Abs. 1, Satz 1 sowie vor der Brück [5].

2.3 Begriffsbestimmungen

2.3.1 Datenschutz und Datensicherheit

Im Gesamtkomplex, der in den vorhergehenden Abschnitten mit "Datenschutz und Datensicherheit" bezeichnet wurde, gibt es eine Fülle von Begriffsbestimmungen, die sich nur teilweise überdecken und manchmal sogar widersprechen.³⁵

Im Jahre 1974 haben das US-amerikanische National Bureau of Standards (NBS) und die Association for Computing Machinery (ACM) eine gemeinsame Definition der Begriffe "security", "privacy", "confidentiality" und "integrity" herausgegeben.³⁶ Es scheint aber nicht möglich zu sein, eine eindeutige Beziehung zwischen diesen Wörtern und deutschen Begriffen herzustellen, zumal die getroffenen Vereinbarungen nicht in allen Punkten befriedigen können: der Begriff "security" erscheint allzu allgemein gefaßt; "privacy" wird im Sinne von "Privatsphäre" benutzt - im Gegensatz zu vielen Verfassern³⁷ und Cassel's New German Dictionary, die den Begriff in etwa mit "Geheimhaltung" gleichsetzen.

Die Arbeitsgruppe 4 der International Medical Informatics Association (IMIA) - eine Special Interest Group der IFIP - spezifiziert u.a. die Begriffe "data protection", "data security", "usage integrity", "confidentiality", "file protection" usw.³⁸

Wulf et al. [80] dagegen unterscheiden zwischen Sicherung als technisches Gebilde und Sicherheit als Philosophie.³⁹

Im deutschsprachigen Raum geben Kassel und Strnad [34] folgende Definition für die in den bisherigen Abschnitten "naiv" verwendeten Begriffe:

- "Datenschutz

- ist im engeren Sinne gemäß Bundesdatenschutzgesetz die Aufgabe, durch den Schutz der personenbezogenen Daten vor Mißbrauch bei der Datenverarbeitung der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken;
- ist im weiteren Sinne die Aufgabe, durch den Schutz der Daten vor Mißbrauch in ihren Verarbeitungsphasen der Beeinträchtigung fremder und eigener Belange zu beugen."

- "Datensicherheit

ist das Ziel bzw. das Ergebnis des Einsatzes geeig-

³⁵ Greiller, Überla [23], Griesser [27], Martin [46], Saltzer, Schroeder [62] u.a.m.

³⁶ In leicht modifizierter Form zitiert bei Hoffman [31], Introduction.

³⁷ Z.B. Petersen, Turn [50], Saltzer, Schroeder [62].

³⁸ Griesser et al. [28], Abschnitte 1.1 und 5.3.

³⁹ "... protection is a mechanism, security is a policy ..."

neter und ausreichender Maßnahmen der Datensicherung, die eine wesentliche Voraussetzung sind, um einen gezielten Datenschutz zu gewährleisten... . Datensicherheit ist allerdings über diesen Aspekt der technischen und organisatorischen Datenschutz-Unterstützung hinaus der DV-technische Begriff für einen angestrebten Zustand, in dem Daten, Programme, DV-Verfahren aber auch Anlagen gegen Mißbrauch, Verfälschung, Verlust oder Zerstörung gefeit oder durch geeignete Vorkehrungen wiederherstellbar (reproduzierbar) sind".

- der Begriff *Datensicherung*, der der Datensicherheit zugrundeliegt, wird definiert als
 "die technisch-organisatorische Aufgabe, die Sicherheit von Datenbeständen und Datenverarbeitungsabläufen zu gewährleisten, d.h. insbesondere zu erreichen, daß
 - der Zugriff zu Daten nur berechtigten Personen möglich ist,
 - keine unerwünschte bzw. unberechtigte Verarbeitung von Daten erfolgt,
 - die Daten bei der Verarbeitung nicht verfälscht werden,
 - die Daten reproduzierbar sind."

Es ist beachtenswert, daß diese letzte Definition weit über die im Rechenzentrumsbetrieb landläufige Bedeutung des Begriffs "Datensicherung" hinausgeht, die nur das Erstellen und Lagern von Kopien betrifft, um den letzten Punkt der umfassenderen Definition (Reproduktionsfähigkeit) zu ermöglichen. Ein weiterer Vorteil dieser Begriffsbestimmungen ist, daß sie streng unterscheiden zwischen Aufgaben, Zielen und Maßnahmen, während diese Differenzierung bei den meisten Definitionen eher verschwommen ist.⁴⁰

Obwohl auch die Definitionen von Kassel und Strnad nicht in allem konsistent sind (nicht sein können?⁴¹), sollen sie den weiteren Ausführungen zugrundegelegt werden; denn es ist hier von Vorteil, daß der Datenschutzbegriff explizit auf den (versehentlichen oder absichtlichen) *Mißbrauch* bezogen wird. Da es in dieser Arbeit wesentlich um die Verhinderung des Mißbrauchs geht, wird von nun an hauptsächlich von Datenschutz in diesem Sinn die Rede sein.

⁴⁰ Bei Griesser et al. [28], Abschnitt 5.3 findet man beispielsweise
 "DATA SECURITY: the *result* achieved through ...
 Synonymous to usage integrity.
 USAGE INTEGRITY: ... the *measures* taken to prevent ...
 Synonymous to data security."

⁴¹ Der übergeordnete Begriff Datensicherheit stellt Forderungen, die stellenweise zu Konflikten führen; so stellt die Datensicherung im landläufigen Sinn eine erhebliche Gefahr für den Datenschutz dar, während dieser die Rekonstruktion zerstörter oder verfälschter Daten empfindlich behindern kann.

2.3.2 Gefährdungen

In der einschlägigen Literatur findet man eine kaum Überblickbare Anzahl verschiedener Klassifikationen der Gefährdungen, denen Datensicherheit und Datenschutz ausgesetzt sind. Griesser [27] unterscheidet beispielsweise:

- | | | |
|--|---|-------------------------------------|
| - Zerstörung ⁴² | | führt zu Datenverlust |
| - Manipulation, Verfälschung | | führt zu ungültigen Daten |
| - unbeabsichtigter Zugriff | | führt zu unbeabsichtigtem Mißbrauch |
| - Diebstahl von Datenträgern | } | bedeutet absichtlichen Mißbrauch |
| - Diebstahl des Inhalts von Datenträgern | | |
| - unberechtigter Zugriff | | |

Lampson [41] dagegen, dessen Hauptsorge der Schutz eigener Daten vor Verrat durch fremderstellte, nicht vertrauenswürdige Programme oder Prozeduren ist, unterscheidet nach den benutzten Datenwegen zwischen:

- Ablegen einer Information in unzulässigen (d.h. anderweitig zugreifbaren) Speicherbereichen,
- Ausnutzung legaler, notwendiger Datenwege, um unzulässig Informationen aus einem geschlossenen Bereich hinaus zu übertragen⁴³,
- Ausnutzung von Systemeigenschaften, die nicht als Datenkanäle gedacht sind, um Informationen preiszugeben ("verdeckte Kanäle"⁴⁴).

Diese Aufzählung, die sich beliebig fortsetzen ließe, möge genügen, um die unterschiedlichen Betrachtungsweisen deutlich zu machen. Für die Ziele dieser Ausführungen ist es beispielsweise unerheblich, ob ein Mißbrauch von Daten absichtlich erfolgt oder nicht; da ferner der Verarbeitungsschutz - wie noch zu zeigen sein wird - gerade die Vertrauenswürdigkeit der eingesetzten Programme erhöhen soll, ist auch die Einteilung von Lampson hier von untergeordneter Aussagekraft. Die folgenden fünf Kategorien dagegen sind geeignet, sowohl die Hauptziele dieser Arbeit herauszuheben, als auch darzustellen, in welchen Bereichen die

⁴² Hinzu kommen andere, der Zerstörung nahestehende Wege, Daten unbrauchbar zu machen; so kennen wohl in jedem Rechenzentrum mehrere Mitarbeiter mindestens eine Methode, das Betriebssystem zum "Absturz" zu bringen und die Verarbeitung beliebiger Daten somit zu verhindern.

⁴³ Es könnte etwa eine fast unmerkliche Änderung des Inhalts der Accounting-Sätze Information verraten.

⁴⁴ "Covert channels"; als Beispiel wird angeführt, daß die für aufeinanderfolgende Transaktionen benötigte Verweilzeit eine Nachricht kodieren kann, wenn unter definierten Umständen eine künstliche Verlängerung eingefügt wird.

technische Lösungen keinen Erfolg versprechen, damit das von Saltzer und Schroeder befürchtete falsche Vertrauen (s. Abschnitt 1) nicht aufkommt:

- Zerstörung/Verhinderung,
- Daten-Diebstahl,
- unberechtigte Systembenutzung,
- unberechtigter/unbeabsichtigter Datenzugriff und
- unberechtigte Verarbeitung.

Bevor diese Begriffe in den folgenden Unterabschnitten erläutert und eingeordnet werden, muß jedoch noch eine grundsätzliche Feststellung getroffen werden. Auch im Bereich des Datenschutzes und der Datensicherheit gibt es, wie in jedem anderen technischen Bereich, keine *absolute* Lösung gegen die Gefährdungen. Man kann mit entsprechendem Aufwand ein beliebiges Maß an wahrscheinlicher Sicherheit erreichen; doch muß der Preis (Kosten, Unannehmlichkeiten für die Anwender usw.) in einem angemessenen Verhältnis zum Wert der Daten stehen. Die Sicherheit der Daten kann folglich einer Kosten/Nutzen-Analyse unterzogen werden. Dies gilt selbstredend auch für einen potentiellen "Feind": Die notwendige Apparatur, Rechen- und Arbeitszeit, die statistisch zu erwartende Dauer bis zum Erfolg eines versuchten "Angriffs" usw. können mit dem zu erzielenden Nutzen bzw. Schaden in Beziehung gesetzt werden;⁵ selbstverständlich ist der Nutzen für einen Eindringling gleich Null, wenn die Beschaffung einer Information länger braucht, als sie aktuell ist oder geheimgehalten wird.

Besonders kostspielig in diesem Sinn sind sicher die Ausnutzung verborgener Kanäle (s.o.) sowie der Schutz dagegen; doch dürften solche Techniken eher im militärisch/geheimdienstlichen Umfeld als bei der personenbezogenen Datenverarbeitung zu befürchten sein und können deshalb hier vernachlässigt werden.

2.3.2.1 Zerstörung/Verhinderung

Unter dem Begriff "Zerstörung/Verhinderung" soll verstanden werden, daß Daten oder die zu ihrer Verarbeitung erforderlichen Geräte, Programme oder Infrastrukturen (Strom, Klima usw.) dauernd bzw. vorübergehend, vor allem aber *ungezielt*^{4 6} unbenutzbar gemacht werden. Dabei ist die Dauer der Verhinderung, die eine Wirkung erzielt, welche in den Folgen einer Zerstörung gleichkommt, von der jeweils betroffenen Aufgabe abhängig. Die Verzögerung des Drucks einer wissen-

^{4 5} S. z.B. Purdy [55] sowie Saltzer und Schroeder [62].

^{4 6} Der Begriff "ungezielt" wird hier in dem Sinn verwendet, daß das Ereignis globale, nicht auf bestimmte interessierende Datenbestände eingeschränkte Wirkung hat. Die *gezielte* Zerstörung (absichtliche Löschung) einzelner Daten oder Datenbestände dagegen muß als *unberechtigter Zugriff* (s.u.) angesehen werden.

schaftlichen Arbeit um Stunden oder Tage wird - bei allem Ärger - in der Regel geringere Probleme aufwerfen, als ein um Größenordnungen kürzeres Ausbleiben von Ergebnissen in der Flugsicherung oder in der Steuerung eines Kraftwerks.

Zerstörung und Verhinderung können ihre Ursachen in Katastrophen, technischem Versagen der Apparate oder Programmfehlern im weitesten Sinn haben. Es sei dahingestellt, ob diese auf Unglück, Fahrlässigkeit, Sabotage oder etwa Streik, Epidemien o.ä. beruhen. Gegen Zerstörung/Verhinderung versucht man sich meist durch bauliche, technische oder organisatorische Maßnahmen zu schützen. Von besonderer Bedeutung sind beispielsweise

- die Lage eines Rechenzentrums innerhalb eines Gebäudes,
- die Verwendung undurchsichtiger und/oder schuß- und explosionssicherer Glasscheiben,
- automatische Feuer- und Einbruch-Alarmanlagen,
- Redundanz in der Apparatur (mehrere, gegenseitig austauschfähige Prozessoren, Steuerungen o.ä., Multiprozessoren, mehrfache, getrennte Datenwege zwischen wichtigen Konfigurationsbestandteilen usw.),
- minimale Zutrittsberechtigung.

Da eine längerfristige oder (bei Daten) endgültig wirkende Zerstörung - wie bereits erwähnt - nicht völlig ausgeschlossen werden kann, ist es allgemeine Praxis, eine "Datensicherung" im herkömmlichen Sinn durchzuführen. D.h. daß eine oder mehrere Kopien der Datenbestände in einem möglichst aktuellen Zustand an gesicherten Orten aufbewahrt werden, die mit hoher Wahrscheinlichkeit nicht (alle) durch dasselbe Zerstörungsereignis in Mitleidenschaft gezogen werden. Ferner kann man durch Absprachen oder Verträge (Teilverfügbarkeit auf) Ausweichanlagen bereithalten; dadurch werden die Auswirkungen der Zerstörung von Anlagen an die der vorübergehenden Verhinderung angenähert.

Durch Zerstörung/Verhinderung wird in erster Linie die Datensicherheit bedroht; es ist deshalb nicht verwunderlich, daß die Anlage zu §6, Abs. 1 Satz 1 BDSG keine Kontrollen nennt, die unmittelbar gegen diese Gefährdung gezielt sind; allenfalls können die Zugangskontrolle und die - extrem vage formulierte - Organisationskontrolle mittelbar Schutz bieten.

2.3.2.2 Daten-Diebstahl

Unter dem Begriff "Daten-Diebstahl" sollen hier drei Tatbestände zusammengefaßt werden:

- der unbefugte, körperliche Transport von Datenträgern⁴⁷ aus dem Schutzbereich,

⁴⁷ Dieser Begriff schließt auch Eingabeformulare, Listen, Speicherabzüge usw. sowie Kopien derselben ein.

- das *passive* Abhören von Leitungen oder Streufeldern anderen Ursprungs,
- das "Ausspionieren" von Passwörtern und dergleichen (z.B. durch Ausnutzen des Vertrauens oder der Sorglosigkeit von Kollegen⁴⁸).

Der Datendiebstahl zielt zunächst einseitig gegen den Geheimhaltungsaspekt des Datenschutzes; beim passiven Abhören und beim "Ausspionieren" kann allerdings auch eine unberechtigte Systembenutzung Ziel und Auswirkung sein, wie in Abschnitt 3.3 noch gezeigt werden soll. Gegen Datendiebstahl wird in der Praxis meist durch bauliche und organisatorische Maßnahmen vorgebeugt. Bei empfindlichen Daten empfiehlt sich auch eine Chiffrierung⁴⁹. Dies gilt besonders bei der Datenübertragung über große Entfernungen unter Ausnutzung nicht kontrollierbarer Kanäle, wie sie immer häufiger vorkommt. Aber in Extremfällen kommt sie auch als "zweite Verteidigungslinie" in Frage, um ggf. doch entwundene Datenträger nicht oder sehr schwer auswertbar zu machen. Allerdings muß der für die Chiffrierung/Dechiffrierung erforderliche, nicht unerhebliche Aufwand im Sinne einer Kosten/Nutzen-Analyse (s.o.) besonders sorgfältig gegen den Wert der Daten, ihre Aktualitätsdauer und die Wirksamkeit der primären Schutzmaßnahmen abgewogen werden.

Im Bereich der personenbezogenen Datenverarbeitung verstößt die Möglichkeit zum Datendiebstahl nach der Terminologie der Anlage zu §6 Abs. 1 Satz 1 BDSG gegen die Abgangskontrolle und die Transportkontrolle; der Datendiebstahl kann aber, wie angedeutet, auch als Mittel zum Angriff gegen die Benutzerkontrolle eingesetzt werden.

2.3.2.3 Unberechtigte Systembenutzung

Unter dem Begriff "unberechtigte Systembenutzung" soll verstanden werden, daß eine nicht autorisierte Verbindung zwischen einem Benutzer und einem DV-System hergestellt wird. Dabei ist es irrelevant, ob dieser Mißstand darauf beruht, daß ein nicht berechtigter Benutzer (der auch ein anderes DV-System sein kann) Zugriff zu einem DV-System erlangt, oder ob ein berechtigter Anwender, ohne es zu merken, an ein falsches (subversives) DV-System angeschlossen wird, und diesem in gutem Glauben schutzwürdige Informationen mitteilt. Um der Gefahr der nicht autorisierten Systembenutzung zu begegnen, sind bauliche oder organisatorische Maßnahmen meist wenig nützlich; denn im Zuge der allgemein zu beobachtenden Dezentralisierung von DV-Leistungen und im Zeitalter offener Kommunikationsnetze ist es nur in Sonderfällen noch akzeptabel, alle Datenendgeräte

⁴⁸ Man kann die Hemmschwelle kaum überschätzen, die zu überwinden ist, um beispielsweise einen Bildschirm bewußt in Gegenwart eines Kollegen oder gar Vorgesetzten zur Eingabe eines Passworts abzudunkeln; s. Saltzer [61].

⁴⁹ Hoffman [31], [32] sowie Martin [46].

in einem geschützten Bereich unterzubringen - von den Möglichkeiten der Rechner-Rechner-Verbindung ganz zu schweigen.

Vordergründig besteht der Schutz gegen unberechtigte Systembenutzung darin, eine Kontrolle über den Verbindungsaufbau auszuüben; hierzu wird in Abschnitt 3.3 mehr zu sagen sein. Es sind jedoch auch Verfahren bekanntgeworden, mit deren Hilfe eine bestehende, legale Verbindung mißbraucht werden kann.⁵⁰ Solche Methoden sind zwar sehr aufwendig und erfordern im allgemeinen den Einsatz eines eigenen, leistungsfähigen Rechners; sie versprechen jedoch auch großen Nutzen: man denke nur daran, aktiv und unentdeckt am Dialog des Systemverwalters teilhaben zu können! Zum Schutz gegen solche aktiven Abhörpraktiken werden in erster Linie - wie gegen das passive Abhören - Chiffrierungs-Techniken eingesetzt; denn andere Schutzmaßnahmen, die bislang gezielt gegen diese Gefährdung erdacht wurden, sind alle mehr oder weniger impraktikabel.⁵¹

Neben den auf den illegalen Benutzer gezielten Maßnahmen ist es auch möglich, die Benutzung der Endgeräte selbst auf bestimmte Anwendungsbereiche o.ä. zu beschränken. Dies ist jedoch offensichtlich eine "zweite Verteidigungslinie", die die Sicherung des Verbindungsaufbaus und die Abhörabwehr keinesfalls überflüssig macht, sondern lediglich ergänzt.

Auf personenbezogene Daten bezogen ist der Schutz vor unberechtigter Systembenutzung eine Realisierung der Benutzerkontrolle nach Anlage zu §6 Abs. 1 Satz 1 BDSG.

2.3.2.4 Unberechtigter/unbeabsichtigter Datenzugriff

Unter "unberechtigtem/unbeabsichtigtem Datenzugriff" sind all die Fälle zu verstehen, bei denen ein (legaler) Systembenutzer im weitesten Sinn lesend oder verändernd auf Daten zugreift, die er nicht in der vorliegenden Art bearbeiten darf. Vom eigentlichen "Lesen" getrennt kann man das "Ausführen" als andersartigen Zugriff behandeln; ebenso kann der weite Begriff "Verändern" differenziert werden, z.B. in

- Hinzufügen,
- Überschreiben (Verändern im engeren Sinn),
- Löschen (von Einzeldaten oder einer ganzen Datei),
- Erzeugen (einer neuen Datei) oder
- Verändern von Berechtigungen.

⁵⁰ Bei dem sogenannten "piggy-back"-Verfahren werden beispielsweise fremde Dialogschritte in die Denkpausen des berechtigten Anwenders eingekoppelt.

⁵¹ Man hat beispielsweise vorgeschlagen, den "strengen" Dialog, bei dem die Flußrichtung der Nachrichten stets wechseln muß, zu erzwingen; diese Maßnahme vereitelt jedoch i.allg. jede Art von gezielter Programmunterbrechung vom Datenendgerät aus - eine besonders in der graphischen Datenverarbeitung häufige Arbeitsweise.

Für jede dieser diversen Zugriffsformen können eigene Berechtigungen definiert werden, die zu beachten sind. Selbstverständlich treten diese Probleme nicht auf, wenn das gesamte DV-System nur die Daten eines einzigen Anwenders enthält und keine Verbindung nach außen besteht. Sobald jedoch die Daten und Programme mehrerer unterschiedlicher Benutzer gleichzeitig im System zugreifbar sein können, müssen Hard- und/oder Software Mittel bereithalten, um Übergriffe zu verhindern. Diese Problematik und die Beschäftigung mit ihr ist deshalb tief verwurzelt in der Entwicklungsgeschichte allgemeiner Betriebssysteme für "Multiprogramm-Betrieb"; viele der in Abschnitt 3 zitierten Stellen befassen sich primär mit allgemeinen Betriebsystemfragen. Aus dem Gesagten dürfte klar hervorgehen, daß bauliche oder organisatorische Maßnahmen ungeeignet sind, um gegen den unberechtigten/unbeabsichtigten Datenzugriff zu schützen.

In der Terminologie der Anlage zu §6, Abs. 1 Satz 1 BDSG handelt es sich bei der Verhinderung des unberechtigten/unbeabsichtigten Datenzugriffs um die Zugriffskontrolle.

2.3.2.5 Unberechtigte Verarbeitung

Die "unberechtigte Verarbeitung" schließlich betrifft den Fall, daß ein autorisierter Benutzer Daten, zu denen er legal zugreifen darf, in unberechtigter Weise verarbeitet. Schneider [64] spricht in diesem Zusammenhang von "nicht legitimiertem" Umgang mit Daten - im Gegensatz zum nicht legitimen, d.h. unberechtigten Datenzugriff.

Um sich dieser Gefahr bewußt zu werden, muß man bedenken, daß gerade die Spezialisten der EDV in der Lage sind, selbst Programme zu entwickeln, die unter Ausnutzung der Privilegien, die ihnen Schöpfern aus ihrer Stellung und Aufgabe heraus zugestanden werden müssen, unstatthafte Verarbeitung durchführen. In diese Kategorie gehören viele Ausprägungen der Computer-Kriminalität.^{5,2}

Ein Sonderfall dieser Problematik ist bei umfangreichen, interaktiv zu verwendenden Datenbanken feststellbar. Hier haben die einzelnen Felder im allgemeinen unterschiedliches Schutzbedürfnis; der in seinen Zugriffsrechten eingeschränkte Benutzer muß aber dennoch bedient werden können, wenn irgendwelche, darin gespeicherten Daten seinem Verfügungsreich angehören. Dann muß das Datenbanksystem (bzw. ein darauf aufgesetzter Transaktionsmonitor oder dergleichen) im allgemeinen Routinen zur Berechtigungskontrolle enthal-

^{5,2} Industrie-Spionage durch leitende Angestellte, militärischer Verrat durch hohe Offiziere, Sabotage usw.; vom Rechenzentrumsleiter einer Großbank wurde einmal gesagt, seine größte Sorge müsse es sein, was seine höchstqualifizierten und somit höchstprivilegierten Mitarbeiter mit den ihnen verfügbaren Daten "anstellen" könnten.

ten, um intern die erforderlichen Schutzfunktionen zu verwirklichen.⁵³ Es besteht aber die weitere Einschränkung, daß

- entweder das Datenbanksystem
 - als selbständiger Prozeß ablaufen muß, der Zugriffsrechte besitzt, wie sie zum Lesen der sensitivsten, in der Datenbank enthaltenen Daten entsprechen,
 - seine Aufträge über Interprozeß-Kommunikation o.ä. erhalten muß und
 - die Ergebnisse - sofern der Auftrag einer Befugnisprüfung standhielt - auf demselben Weg zurückmeldet;
- oder die Datenbank (in toto) auch für den genannten Benutzer mit eingeschränkten Rechten zugreifbar sein muß.

Die erste Lösung führt zu den bekannten Serialisierungseffekten, die die Effizienz eines Systems entscheidend beeinträchtigen können. Im zweiten, durchaus anzutreffenden Fall⁵⁴ aber ist eine Sicherheit gegen unberechtigte Verarbeitung nur gegeben, wenn sichergestellt werden kann, daß die Datenbank mit anderen Mitteln (Programmen) nicht zugreifbar ist.

In die Kategorie der unberechtigten Verarbeitung ist ferner eine Schwierigkeit einzuordnen, die als "Versions-Problem" bezeichnet werden soll. Darunter ist zu verstehen, daß ein zugelassenes Programm verändert wird, sei es, daß der für die Erstellung und Pflege zuständige Mitarbeiter "schnell mal" eine neue, verbesserte (aber vielleicht doch nicht ausreichend überprüfte) Version unter Umgehung der Revisionsinstanzen einführt,⁵⁵ sei es, daß ein absichtlich "subversives" Verhalten unterschoben wird.

Besonders gravierend sind die Folgen einer unberechtigten Verarbeitung oft dann, wenn diese eine Übermittlung der Daten in einen anderen Arbeitsbereich und/oder zu einem anderen DV-System bewirkt.⁵⁶ Es liegen offensichtlich gerade Befürchtungen dieser Art dem bereits erwähnten Streit um das Volkszählungsgesetz 1983 und vielen anderen Vorbehalten gegen die personenbezogene Datenverarbeitung zugrunde.

⁵³ Griese und Plesch [25], Petersen et al. [50] u.a.m.

⁵⁴ S. beispielsweise Zeiler [84]; es handelt sich zugegebenermaßen um einen Grenzfall zum unberechtigten Datenzugriff; er wird aber an dieser Stelle angeführt, weil die Funktion des Datenbanksystems im Vordergrund steht, und weil ein solcher Fall im Zuge der Behandlung des Verarbeitungsschutzes in Abschnitt 4 betrachtet wird.

⁵⁵ Petersen, Turn [51]; dies ist eine in der Praxis leider häufig anzutreffende Verhaltensweise, die sich immer wieder verhängnisvoll auswirkt (vorwiegend als Bedrohung der Datensicherheit), und der - vor allem in kleinen Rechenzentren und beim Einsatz von Kleincomputern - nur schwer beizukommen ist.

⁵⁶ Z.B. Patientendaten über einen Krankenhausangestellten in die eigene Personalabteilung (ggf. im selben Rechner!), Krankenakten an zentrale Polizeibehörden oder Gehaltsdaten an kommerzielle Unternehmen.

Im medizinischen Bereich ist ein weiterer Aspekt von besonderer Bedeutung, wenn es gelingt, die unberechtigte Verarbeitung zu verhindern: in Abschnitt 2.1.2 wurde bereits erläutert, daß es in vielen, interessanten Fällen möglich ist, anonymisierte Daten, wie sie z.B. medizinisch-statistischen Querschnittsuntersuchungen oder epidemiologischen Studien zugrunde liegen, mit mehr oder weniger großem Aufwand zu "entanonymisieren", d.h. in die ursprünglichen, personenbezogenen Daten zurückzuführen. Sofern dies nicht dem legitimen Arbeitsziel dient, sondern vielmehr zum Geheimnisverrat mißbraucht wird, handelt es sich selbstredend um eine unberechtigte Verarbeitung. Gelingt es, dies zuverlässig zu verhindern, so entfallen damit auch weitestgehend alle Vorbehalte gegen die Verwendung dieser Daten in einer Umgebung, die den Zugriff selbst nicht oder nicht streng schützt. Voraussetzung hierfür ist allerdings, daß solche Daten nicht kopiert werden können; denn sonst wäre die Kopie gegen Entanonymisierung nicht geschützt. Die Vervielfältigung von Daten ist jedoch - wie in Abschnitt 4.2.2.1 näher ausgeführt werden soll - ebenfalls als eine Form der Verarbeitung anzusehen, die verhindert werden muß, wenn sie dem berechtigten Verarbeitungsziel abträglich ist.

Die Verhinderung der unberechtigten Verarbeitung betrifft bei personenbezogenen Daten die Speicherkontrolle und die Auftragskontrolle nach der Definition der Anlage zu §6, Abs. 1 Satz 1 BDSG. Ferner sind Übermittlungskontrolle und Eingabekontrolle betroffen, wenn das Betriebssystem nicht die Möglichkeit einer selbsttätigen Zugriffsprotokollierung vorsieht.

2.3.3 Gegenüberstellung der Gefährdungen zu den gesetzlichen Vorschriften

Für personenbezogene Daten ist in den voranstehenden Abschnitten jeweils eine Zuordnung der erläuterten Gefährdungskategorie zu den Kontrollen nach der Anlage zu §6, Abs. 1 Satz 1 BDSG angegeben worden. Tabelle 1 faßt diese Angaben zusammen, wobei nach der Art der Beziehung unterschieden wird: ob beispielsweise das Eintreffen eines Gefährdungsereignisses eindeutig auf die Nichteinhaltung einer Kontrolle schließen läßt, ob umgekehrt das Versagen einer Kontrolle ein gewisses Gefährdungsereignis ermöglicht usw. Der zutage tretende Mangel an Eindeutigkeit bei dieser Zuordnung ist auf die bereits in Abschnitt 2.2 festgestellte Überschneidung einzelner Kontrollforderungen und auf ihre unterschiedliche Qualität zurückzuführen. Dagegen sind die definierten Gefahren gleichartig, insofern als sie jeweils eine Tätigkeitsklasse bestimmen, die den Datenschutz bedroht, und sie weisen keine oder nur minimale Überschneidungen auf.

Hervorzuheben ist die Bedeutung der Tabelleneinträge "1" und "2". Die Erläuterung weist diese Fälle als besonders kritisch aus; denn die betreffende gesetzliche Forderung ist in diesen Fällen nicht sicher erfüllbar, wenn das ange-

gebene Ereignis eintreten kann; ohne hinreichenden Schutz vor der jeweiligen Gefahr ist die Kontrollforderung nicht erfüllbar. Solche Einträge betreffen vor allem die rechner-internen Aspekte, wie sie Speicher-, Benutzer-, Zugriffs-, Übermittlungs-, Eingabe- und Auftragskontrolle zum Ziel haben, und es verwundert deshalb nicht, daß sie den Gefährdungen zugeordnet sind, die nach dem bisher Gesagten mit DV-technischen Mitteln verhindert werden können und müssen. Speziell auf den in Abschnitt 4 näher zu behandelnden Ver-

	Zerstörung/ Verhinderung	Daten—Diebstahl	unberechtigte System—Benutzung	unberechtigter Daten—Zugriff	unberechtigter Verarbeitung
Zugangskontrolle	3	3	4		
Abgangskontrolle		3			
Speicherkontrolle			1	1	1
Benutzerkontrolle			1		
Zugriffskontrolle				1	
Übermittlungskontrolle		3			2
Eingabekontrolle				3	2
Auftragskontrolle					1
Transportkontrolle		3		3	3
Organisationskontrolle	3	(3)	3	(3)	(3)

Die eingetragenen Ziffern haben folgende Bedeutung:

- 1: die Kontroll-Forderung wird bei Eintreffen des Gefahrenereignisses verletzt; sie ist nicht sicher erfüllbar, wenn das Gefahrenereignis eintreffen kann;
- 2: wie 1, es sei denn, das Betriebssystem sieht eine automatische Protokollierung aller Zugriffe vor;
- 3: die Kontroll-Forderung kann bei Eintreffen des Gefahrenereignisses verletzt worden sein; die Kontrolle soll der Gefährdung gezielt entgegenwirken;
- 4: wie 3, gilt jedoch nur, wenn für spezielle Benutzerkennungen nur Datenendgeräte zugelassen sind, die sich im Sicherheitsbereich befinden.

Tabelle 1: Kontrollen nach BDSG und Gefährdungen

arbeitungsschutz bezogen, ist die ausschlaggebende Tatsache klar erkennbar, daß weder die - in ihrem Stellenwert als zentral anzusehende - Speicherkontrolle, noch die Auftragskontrolle gewährleistet werden können, wenn die unberechtigte Verarbeitung nicht zuverlässig verhindert wird. Dasselbe gilt für die Eingabekontrolle und für die - im Zeitalter großer, offener Netze besonders aktuelle - Übermittlungskontrolle, die im Gegensatz zu den zuvorgenannten Kontrollen nicht so sehr der Verhinderung des Mißbrauchs dienen, als vielmehr einer nachträglichen Überprüfung, sofern das eingesetzte Betriebssystem nicht eine Option bereithält, alle Zugriffe zu ausgewählten Datenbeständen selbsttätig in auswertbarer Form zu protokollieren. Die Gefahr der unberechtigten Verarbeitung betrifft mehr gesetzliche Kontrollen als irgend eine der anderen.

3. TECHNISCHE STRATEGIEN UND WERKZEUGE ZUR REALISIERUNG DES DATENSCHUTZES

Ein sicheres Betriebssystem liegt nach einer Definition von Popek et al. [54] dann vor,

*wenn es sich schlüssig als sicher erweisen läßt in dem Sinn, daß die für eine heterogene Anwenderpopulation gespeicherten Informationen vor unberechtigten Zugriffen und Änderungen geschützt werden, auch wenn dies fachmännisch versucht wird.*⁵⁷

Die explizite Qualifizierung der Anwenderpopulation als heterogen macht die bereits erwähnten Tatbestände deutlich,

- daß der DV-technische Datenschutz als kein Thema betrachtet wird in einem System, zu dem nur ein Anwender (eine geschlossene Anwendergruppe) Zugang hat, der auch Besitzer der Daten ist;
- daß der in Abschnitt 2.3.2.3 geforderte Schutz gegen unberechtigte Systembenutzung Grundlage jedes sicheren Systems ist.

Zweifellos ist die schwerste Aufgabe, die sich aus dieser Definition ergibt, die Forderung, daß die Sicherheit "schlüssig erwiesen" werden muß. Da ein solcher Beweis bislang nirgends oder nur recht bruchstückhaft erbracht werden konnte,⁵⁸ und auch die in Abschnitt 4 darzustellende Realisierung des Verarbeitungsschutzes keinen Anspruch in dieser Hinsicht erhebt, wird es gut sein, zunächst die wichtigsten, weniger strengen aber allgemein bewährten Grundsätze aufzuführen, wie sie in den letzten 15 Jahren mehr oder weniger pragmatisch entwickelt und beschrieben wurden. Selbstredend gibt es auch in diesem Punkt fast ebenso viele unterschiedliche Darstellungen,⁵⁹ wie es Behandlungen dieses Themas gibt. Deshalb und aufgrund der eher grundlegenden Funktion des folgenden Abschnitts wird kein Versuch unternommen, alle geschilderten Wege detailliert zu erläutern, sondern versucht, das Prinzipielle herauszuarbeiten. Für genauere Angaben wird auf die im Text angegebene Literatur verwiesen.

⁵⁷ "... conclusively shown that the information stored on behalf of a heterogeneous user population was safely protected from unauthorized access or modification even in the event of skilled attempts to do so ..."

⁵⁸ Ames und Millen [1], Berson und Barksdale [4], Gold et al. [21], McCauley und Drangowski [47], Millen [48], Popek et al. [52] - [54] berichten von Versuchen, Sicherheitskerne (s. nächsten Abschnitt) zur Realisierung des Informationsschutzes (s. Abschnitt 3.4.3.1) zu implementieren und zu verifizieren. Obwohl sich die meisten auf das "kleine" System UNIX konzentrieren, wird nur die formale Spezifikation, nicht aber die Implementierung als korrekt bewiesen. Die sogenannten "trusted Programs" (s. ebenfalls Abschnitt 3.4.3.1) bleiben praktisch ausgespart.

⁵⁹ Linden [44] nennt sie sogar kontrovers.

3.1 Grundprinzipien

Im Vorfeld der spezifischen Techniken zur Realisierung des Datenschutzes gibt es eine Anzahl grundsätzlicher Forderungen, die aus plausiblen Gründen zu erfüllen sind, wenn diesbezügliche Maßnahmen Aussicht auf Erfolg haben sollen.

Saltzer und Schroeder [62] sowie Hoffman [31] zählen je eine Liste solcher Grundprinzipien für das Entwerfen von Sicherheitsmaßnahmen auf. Die folgende Aufstellung ist als eine Vereinigung dieser beiden Listen anzusehen:

- *Standardmäßige Verarbeitungsverweigerung* ("default to access denial"/"fail safe defaults"): grundsätzlich ist jede Verarbeitung (fremder Daten) zu verweigern; eine Erlaubnis muß explizit erteilt werden.
- *Offengelegte Methodik* ("nonsecret design"): die Sicherheitsverfahren dürfen sich nicht darauf stützen, daß sie selbst geheimlicht werden; es gibt immer Methoden, sie zu analysieren und damit zu Fall zu bringen.
- *Minimal-Befugnisse* ("least privilege"/"need to know"): dem Anwender sollen nur die Befugnisse erteilt werden, die er zur Durchführung seiner Arbeit benötigt.⁶⁰
- *Vollständige Kontrolle* ("complete mediation"): absolut jeder Zugriff zu den geschützten Daten soll die Sicherheitsmaßnahmen durchlaufen.
- *Benutzerfreundlichkeit* ("user acceptability"): die Schutzmaßnahmen dürfen die Arbeit der Anwender nicht übermäßig, d.h. unangemessen im Verhältnis zur einzu-sehenden Schutzforderung, beeinträchtigen, da diese sonst Umgehungen suchen und benutzen werden (sofern die vollständige Kontrolle nicht gelingt) bzw. sie werden das System nur unwillig benutzen oder gar sabotieren.
- *Einfachheit* ("economy of mechanism"): dieses in der Informatik allgemein gültige Prinzip⁶¹ gewinnt besonderes Gewicht, wenn Sicherheitsmaßnahmen nach strengen Kriterien überprüft werden sollen.
- *Verteilte Befugnisse* ("separation of privilege"): bei sehr sensitiven Verarbeitungsvorgängen soll das Zusammenwirken mehrerer, unabhängiger Personen erzwungen werden können. Kein Einziger sollte die Fähigkeit zu

⁶⁰ Das im Ausdruck "need to know" angesprochene, nur bei Bedarf zu vermittelnde Wissen bezieht sich auf den Dateninhalt; es besteht somit kein Widerspruch zum Grundprinzip der offengelegten Methodik und es sollen keine inkompetenten Anwender "herangezuchtet" werden.

⁶¹ Vgl. das Prinzip der "Strukturierten Programmierung" mit den dazuführenden Erkenntnissen über die Unzulänglichkeit menschlichen Denkens; Dijkstra [13]-[15], Infotech [33] u.a.m; s. auch Wulf und Shaw [81].

unbeschränktem Datenzugriff haben.⁶²

- *Minimierung globaler Mechanismen* ("least common mechanism"): die Verwendung systemglobaler Variabler bietet ggf. einen Informationskanal für die unzulässige Übermittlung zu schützender Informationen;⁶³ Funktionen sollten nur soweit unbedingt erforderlich durch den privilegierten Teil des Betriebssystems bereitgestellt werden.

Eine weitere, häufig gestellte Forderung ist die nach einem Gefährdungsprotokoll ("threat monitoring"⁶⁴). Das bedeutet, daß das Eintreffen gewisser Ereignisse gemeldet werden soll, die als *Versuch* gedeutet werden können, das Sicherheitssystem zu umgehen.⁶⁵ Ob solche Meldungen einen unmittelbaren Alarm bei dem für den Datenschutz zuständigen Mitarbeiter auslösen, als Konsolmeldungen erscheinen oder in eine periodisch auszuwertende Datei geschrieben werden, ist eine Frage der Verhältnismäßigkeit.

Die zuletzt genannte Forderung darf nicht verwechselt werden mit der nach lückenloser Zugriffs-Protokollierung ("auditing"⁶⁶). Ein solches Vorgehen kann je nach Sensitivität der Datenbestände nur für den verändernden oder auch für den lesenden Zugriff erforderlich sein. Bezogen auf das Verändern personenbezogener Daten ist diese Forderung identisch mit der Eingabekontrolle der Anlage zu §6 Abs. 1 Satz 1 BDSG. Da es ziemlich aufwendig sein kann, eine solche Protokollierung als selbständige Betriebssystemfunktion zu verwirklichen, wird sie meist auf der Ebene der Datenbank- oder Benutzersoftware durchgeführt. Dies wirft allerdings die Frage nach möglichen Umgehungen auf, die zur unberechtigten Verarbeitung (s. Abschnitt 2.3.2.5) gezählt werden müssen.

Obwohl die aufgezählten Grundprinzipien plausibel sind und sich vielfach bewährt haben, darf nicht übersehen werden, daß ihre Einhaltung allein nicht für die Sicherheit eines Systems bürgt, ebenso wie etwa die Anwendung der Technik der Strukturierten Programmierung nicht automatisch gute Programme erzeugt. Zwar sind aus heutiger Sicht unstrukturierte Programme i. allg. unbefriedigend, und dementsprechend verspricht das Entwerfen eines Sicherheitssystems ohne Berücksichtigung der Grundprinzipien kaum Erfolg; doch gibt es auch genügend Beispiele für strukturierte Programme schlechter Qualität.

⁶² S. Abschnitt 4.5.

⁶³ S. Lampson [41].

⁶⁴ Hoffman [32], Martin [46], Palme [49], Petersen, Turn [51] u.a.m.

⁶⁵ Z.B. Aufruf einer Funktion von einem hierfür nicht zugelassenen Terminal oder mehrfache, zeitlich dicht aufeinanderfolgende Eingaben eines falschen Passworts und dergleichen.

⁶⁶ Das Wort "auditing" wird von manchen Autoren für die Programm-Revision verwendet; es ist deshalb bei der Interpretation jeweils Vorsicht geboten.

Ferner muß deutlich darauf hingewiesen werden, daß die Grundprinzipien nicht gänzlich widerspruchsfrei sind. Als Beispiel betrachte man die Forderung nach Benutzerfreundlichkeit, die zu der nach vollständiger Kontrolle in Konflikt stehen kann: wird etwa in einem Dialogsystem für jede Transaktion eine erneute Eingabe eines Passworts verlangt, um den Mißbrauch eines versehentlich "offengelassenen" Terminals zu verhindern, kann dies zur Folge haben, daß jemand die Intelligenz seines Arbeitsplatzes ausnutzt, um das Passwort automatisch ergänzen zu lassen. Ebenso müssen die Grundprinzipien natürlich im Einzelfall am ggf. resultierenden Effizienzverlust im Sinne einer Kosten-/Nutzen-Analyse gemessen werden.

Diesen Vorbehalten zum Trotz können die bisher genannten Grundprinzipien - genauer: deren Nichteinhaltung - wichtige Hinweise auf Sicherheitsmängel liefern, und jedes Sicherheitssystem wird sich nicht zuletzt an diesem Maßstab beurteilen lassen müssen.

Von fundamentaler Qualität dagegen ist die Forderung nach "Nuklearisierung" ("kernelization") der Datenschutzfunktionen in Betriebssystemen. In allen bekannten, kommerziell vertriebenen Betriebssystemen sind die - mehr oder weniger spärlich ausgelegten - Sicherheitsfunktionen über das gesamte Softwaregebilde verteilt. So kann beispielsweise die Zulässigkeitsprüfung eines Datenzugriffs unter verschiedenen Umständen an verschiedenen Stellen durchgeführt werden oder eine einzelne Prüfung die Zusammenarbeit mehrerer, unabhängiger Funktionen erfordern. Es gibt in der Literatur jedoch viele Belege⁶⁷ dafür, daß eine Zerstreuung der schutzrelevanten Mechanismen in den vielen Modulen eines Betriebssystems nicht nur eine strenge Überprüfung der Funktionstüchtigkeit in der Praxis unmöglich macht; sie zieht vielmehr eine an Sicherheit grenzende Wahrscheinlichkeit nach sich, daß die Schutzbedürfnisse kompromittiert werden. Es ist deshalb in einem strategisch auf Datenschutz und Datensicherheit ausgelegten System erforderlich, daß alle diesbezüglichen Funktionen in einem "Sicherheitskern" oder "Nukleus" ("kernel") zusammengefaßt werden. Ein dermaßen aufgebautes System bezeichnet man als "nuklearisiert". Zur Wahrung des Grundprinzips der Einfachheit sollte dieser Kern möglichst klein gehalten werden und auf keine ihm externen Funktionen des Betriebssystems zurückgreifen. Popek et al. [53] zeigen, daß der Sicherheitskern sogar dem sonst grundlegenden Paging-Algorithmus gegenüber zentral angesetzt werden muß.

Die Nuklearisierung von Betriebssystem-(Teil-)Implementierungen ist die Grundlage für alle Versuche, den Forderungen von Popek et al. [54] nachzukommen;⁶⁸ Sicherheit überprüfbar zu machen. Daß diese Forderung in keinem gängigen Betriebssystem erfüllt ist, ist eine Verletzung der Erkenntnis von

⁶⁷ Z.B. Walter et al. [79].

⁶⁸ S. Einleitung zu Abschnitt 3 und Fußnote 58.

Bates [3], daß allen Sicherheitsmaßnahmen eine Strategie zugrunde liegen muß. Die Komplexität der Betriebssysteme läßt kaum hoffen, daß die historisch gewachsenen Strukturen in absehbarer Zeit revidiert werden könnten. So bleibt die Forderung nach einem nuklearisierten Betriebssystem vorerst unerfüllt.

3.2 Ausweisorientierte und listenorientierte Schutzmechanismen

Saltzer und Schroeder [62] machen darauf aufmerksam, daß so gut wie alle Schutzmechanismen sich in eine von zwei Kategorien einordnen lassen, die als "ausweisorientiert" und "listenorientiert" bezeichnet werden.

Bei den *ausweisorientierten* Techniken besitzt das berechnete "Subjekt" je gesichertem "Objekt" einen - idealerweise fälschungssicheren - "Ausweis" ("ticket") mit dem es seine - ggf. eingeschränkten - Befugnisse belegt. Ein solcher Ausweis kann ein (körperlicher) Schlüssel, eine Plastikkarte, ein geheimes Passwort oder gar eine Eigenschaft des eigenen Körpers sein, wenn das DV-System selbst als zu schützendes Objekt betrachtet wird (s. nächsten Abschnitt); es kann - auf Daten bezogen - auch ein geheimes Datei-Kennwort⁶⁹ sein.⁷⁰ Es gibt aber auch andere, weniger auffällige Formen des Ausweises:

- der Name einer fremden Datei, die nicht weiter geschützt wird,⁷¹
- die bereits eingegebene Benutzererkennung, da die "eigenen" Daten fast immer grundsätzlich verfügbar sind,
- eine Datenstrukturbeschreibung, die die Umwandlung der physikalischen Speicherungsform in logische Information ermöglicht,
- ein Dechiffrierschlüssel.

Diese Aufstellung ließe sich fast beliebig fortsetzen.

Die *listenorientierten* Schutztechniken dagegen verwenden Befugnis-Verzeichnisse. Diese geben an, welche Subjekte auf ein spezifisches Objekt zugreifen dürfen und ggf. mit welchen Befugnissen, bzw. welche Objekte ein Subjekt entsprechend verwenden darf, je nachdem, ob sie dem Objekt oder dem Subjekt beigeordnet sind. Beispiele für solche

⁶⁹ Der oft in dieser Bedeutung verwendete Begriff "Passwort" wird hier vermieden, um eine Verwechslung mit den dem Schutz gegen unberechtigte Systembenutzung dienenden Passwörtern zu verhindern.

⁷⁰ Evans und Kantrowitz [17] schlagen eine quasi-irreversible Verschlüsselung von Pass- und Kennwörtern für die intern gespeicherte Darstellung vor, um sie unfälschbar zu machen.

⁷¹ Ohne Kenntnis der Dateibezeichnung ist in einer Betriebssystem-Umgebung selbstredend kein Zugriff möglich.

Listen sind:

- die Liste der Benutzerkennungen (Subjekte), die berechtigt sind, mit einem System in Verbindung zu treten,
- eine Liste der zur Modifikation einer Datei zugelassenen Benutzer,
- eine Liste privilegierter Programme, die gewisse Schutzmaßnahmen für sich außer Kraft setzen dürfen, um zentrale Aufgaben (z.B. Datensicherung im herkömmlichen Sinn) durchführen zu können,
- eine Liste der Anwender, die ein spezielles Feld in einer Datenbank ansehen bzw. verändern dürfen.

Man beachte, daß die immer wieder vorgeschlagene Umkehrung, Listen mit *nicht* zugriffsberechtigten Subjekten zu führen,⁷² gegen das Grundprinzip der standardmäßigen Zugriffsverweigerung verstößt, ja, daß der Schutz bereits durchbrochen wird, wenn ein neues Subjekt erzeugt wird. Bei listenorientierten Sicherheitssystemen ist es deshalb erforderlich, ein spezielles Listenelement "Alle" zu definieren, wenn die Option, einzelne Objekte unterschiedslos allen Subjekten zur Verfügung zu stellen,⁷³ vorgesehen werden soll. Anderenfalls müßten die Listen solcher "global permissiver" Objekte ebenfalls bei jedem neu hinzukommenden Subjekt erweitert werden - eine nicht effizient durchführbare Aufgabe.

Den ausweis- und listenorientierten Sicherheitssystemen ist gemeinsam, daß eine Kontrollinstanz, "Wächter" oder "Monitor"⁷⁴ genannt, bei jedem - versuchten - Zugriff auf ein geschütztes Objekt eingeschaltet werden muß, welche die entsprechende Berechtigung zu überprüfen hat. Diese Prüfung geschieht aus der Sicht des Subjekts "verdeckt"; der Monitor fängt den Zugriffswunsch selbsttätig ab, und das Subjekt bemerkt dies nur, wenn ihm der Zugriff verwehrt wird. Führt in einem System ein Weg unter Umgehung des Monitors zum Zugriff auf ein zu schützendes Objekt, so kann das System nicht als sicher bezeichnet werden.

Nur selten arbeiten Sicherheitssysteme ausschließlich nach ausweis- oder listenorientierten Prinzipien; denn einerseits bieten Listen einen wesentlich umfangreicheren und flexibleren Schutz, andererseits erfordern sie einen beträchtlich höheren, mit Effizienzverlust einhergehenden Aufwand im Monitor. Oft wird die Wächterinstanz deshalb, nachdem sie die Berechtigung eines Subjekts an Hand einer Liste überprüft hat, diesem einen vergänglichen Ausweis

⁷² S. z.B. Control Data Corporation [6], Kriener, Michels [39].

⁷³ Solche Objekte sind beispielsweise allgemeine Dienstprogramme und -prozeduren, Unterprogramm-Bibliotheken, Benutzerinformations-Dateien usw., die zu den wirkungsvollsten Instrumenten zählen, die moderne Multiprogramming-Systeme so effizient machen.

⁷⁴ Graham, Denning [22], Saltzer, Schroeder [62]; nicht zu verwechseln mit dem Monitor-Begriff von Hoare [30]!

übergeben, um die Prüfung künftig zu beschleunigen?⁷⁵ Dies entspricht, um ein Bild von Saltzer und Schroeder zu verwenden, dem Vorgehen bei einem Kongreß, wenn der Teilnehmer einen Namens-Anstecker erhält, sobald festgestellt wurde, daß seine Anmeldung ordnungsgemäß durchgeführt wurde; dieser Ausweis verschafft ihm Zutritt zu den Veranstaltungen, ohne daß der Saalordner seine Berechtigung nochmals explizit verifizieren oder auch nur auf den Namen schauen müßte. Solche sekundären Mechanismen ziehen sich in der Systemarchitektur oft bis in die Hardware hinein, sind aber für den Anwender selbst nur in den seltensten Fällen erkennbar. Eine weitere Erklärung für die höhere Effizienz der ausweisorientierten Sicherheitstechniken wird Abschnitt 3.4.2 liefern.

3.3 Benutzungsschutz

Unter dem Begriff "Benutzungsschutz" sollen alle Maßnahmen verstanden werden, welche die in Abschnitt 2.3.2.3 dargestellte unberechtigte Systembenutzung verhindern sollen. Dort wurde bereits erwähnt, daß bauliche und organisatorische Mittel als Gegenmaßnahmen nicht in Frage kommen. Die Maßnahmen gegen diese Gefährdung sind also Funktionen der Software und - in der bisherigen Praxis in geringerem Maße - der Hardware. Der Frage des Benutzungsschutzes widmen die allermeisten der speziell den Datenschutz betreffenden Veröffentlichungen breiten Raum?⁷⁶ Unbestritten ist dabei die Feststellung, daß zwei gesonderte Informationen an das System übertragen und von diesem überprüft werden müssen:

- eine "Identifikation", mit der der Partner, der das System benutzen möchte, sich als ein in eine Aufstellung eingetragener "Berechtigter" zu erkennen gibt (Benutzererkennung) und
- eine "Authentifikation" ("authentication"), mit der die Partner sich gegenseitig⁷⁷ glaubhaft machen, der

⁷⁵ Ein solches Vorgehen bedeutet nicht in sich einen Verstoß gegen das Grundprinzip der vollständigen Kontrolle, solange streng auf die Unverwechselbarkeit der temporären Ausweise geachtet wird; allerdings ist eine nachträgliche Zugriffszuordnung kaum mehr möglich.

⁷⁶ Hoffman [31], [32], Martin [46], Purdy [55], Saltzer [61], Wood [80] u.a.m.; so gut wie jede Arbeit über Datenschutz berührt dieses Thema zumindest.

⁷⁷ Es wird verschiedentlich in der angegebenen Literatur darauf hingewiesen, daß es ebenso wichtig wie der gewöhnlich betrachtete Fall der Vorsorge gegen einen unberechtigten Benutzer sein kann, einen berechtigten Benutzer davor zu schützen, daß sich ein subversives System einschaltet und das von ihm als Partner gewünschte simuliert; diese Symmetrie des Schutzbedürfnisses ist bei der Rechner-Rechner-Kopplung besonders einleuchtend und dringend. Dem Verfasser ist allerdings kein reales, nicht-experimentelles Betriebssystem bekannt, das diese gegenseitige Absicherung ("hand shaking") für "normale" Benutzer verwirklicht.

zu sein, für den sie sich ausgeben.

Gerade zur sicheren Authentifikation sind sehr viele Methoden vorgeschlagen worden. Alle haben gemeinsam, daß Information ausgetauscht wird über

- Dinge, die der Partner wissen muß⁷⁸ ("something he knows"),
- Dinge, die der Partner haben muß⁷⁹ ("something he has") und/oder
- Eigenschaften des Partners⁸⁰ ("something he is").

Die primitivste Authentifikationsmethode ist das (einseitig vom Benutzer anzugebende) Passwort, das jedoch als notorisch unsicheres Mittel gilt;⁸¹ dessen leichte Umgehung sogar mehrfach Eingang in die Trivialliteratur gefunden hat,⁸² und das sich aktuell als medienwirksame Schwachstelle erweist.⁸³ Sie ist dennoch fast die einzige, in kommerziellen Systemen eingesetzte Methode; allenfalls wird noch die (ebenfalls einseitige) Verwendung von Schlüsseln oder Identifikationskarten mit Magnetstreifen unterstützt, die jedoch für sich allein wegen der Diebstahlsgefahr und logistischer Schwierigkeiten kaum befriedigen können. Sofern ihr Gebrauch keinen überprüfbaren Nachrichtenfluß zum Partner auslöst, können solche Mittel überhaupt nicht als Authentifikationsverfahren angesehen werden, sondern müssen den organisatorischen Sicherungsmaßnahmen zugeordnet werden.

An dieser Notwendigkeit der Übertragung der Authentifikations-Information wird jedoch die große Gefahr deutlich, die von den passiven Abhörverfahren und dem "Ausspionieren" (s. Abschnitt 2.3.2.2) ausgeht: wird eine solche Information abgefangen, so kann sie später von einem Unberechtigten verwendet werden, um selbst das System zu benutzen. Sofern es sich bei der Authentifikations-Information um

⁷⁸ Hierzu gehören u.a. Passwörter und persönliche/familiäre Daten.

⁷⁹ Schlüssel, maschinenlesbare Plastikkarten usw.

⁸⁰ Das Erkennen solcher Eigenschaften wie z.B. Stimme, Handform oder Fingerabdruck erfordert allerdings einen derzeit meist noch prohibitiven technischen Aufwand.

⁸¹ Der leichten Memorisierbarkeit wegen werden meist Daten aus dem unmittelbaren Lebensbereich des berechtigten Benutzers als Passwort verwendet, die relativ leicht zu erraten sind. Auf diesen und weitere, interessante und umfassend untersuchte Umstände kann in der vorliegenden Arbeit nicht näher eingegangen werden; es wird auf die zitierte Literatur verwiesen, sowie speziell auf Reichertz [56] für einschlägige statistische Untersuchungen.

⁸² Beispielsweise Stout [75].

⁸³ Die bisher bekanntgewordenen, spektakulären Erfolge der "Hacker" (s. Fußnote 7) scheinen alle auf ungeschickte Wahl oder sorglosen Umgang mit Passwörtern durch den Anwender oder das Betriebssystem zurückzuführen zu sein; unter diesem Personenkreis kursieren dem Vernehmen nach regelrechte Passwort-Verzeichnisse!

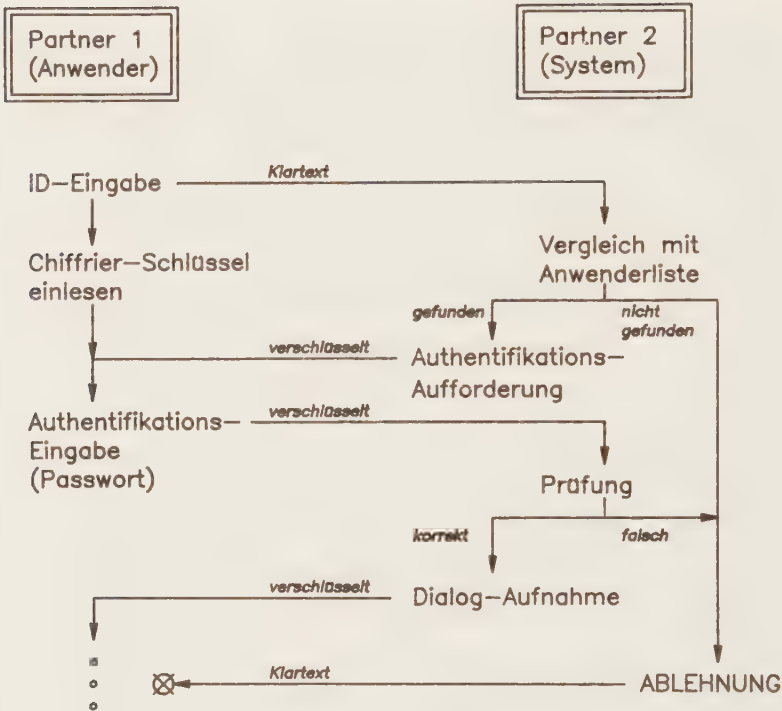


Abb. 2: Authentifikationsmethode nach Feistel

Passwörter handelt, bietet ein häufiger Wechsel einen gewissen Schutz;⁸⁴ idealerweise sollte jedes Passwort nur einmalig zur Authentifikation verwendet werden können.⁸⁵ Bei Schlüsseln, Plastikkarten oder Körpereigenschaften des Benutzers ist ein solcher häufiger Wechsel der Authentifika-

⁸⁴ Das Sicherheitspaket RACF zu OS/VMS von IBM z.B. erzwingt eine periodische Passwortänderung.

⁸⁵ Dem Benutzer können z.B. vorbereitete Listen mit Zufalls-Passwörtern zur Verfügung gestellt werden. Diese Vorgehensweise hat aber zwei gravierende Nachteile:

- eine solche Liste kann nur schwer vor dem "Ausspionieren" bzw. Diebstahl geschützt werden;
- im Fall eines mißlungenen Benutzungsversuchs (Systemabsturz während der Kommunikationseinleitung o.ä.) oder, wenn der Benutzer vergißt, ein bereits benutztes Passwort in seiner Liste zu löschen, ist eine erneute Synchronisation zwischen System und Anwender beschwerlich; im ungünstigsten Fall kann das System einen versuchten Unterschleif diagnostizieren und Alarm schlagen.

tions-Information nur schwer bzw. prinzipiell nicht möglich.

Daß dennoch eine sehr hohe Authentifikationssicherheit erreicht werden könnte, zeigt ein Vorschlag von Feistel⁸⁶ (Abb. 2). Hierzu bedarf es auf der Benutzerseite eines Terminals mit einem Plastikkartenleser o.ä. und ausreichender Intelligenz, um einen Chiffrier-/Dechiffrier-Algorithmus durchzuführen.⁸⁷ Der Identifikations- und Authentifikations-Vorgang spielt sich dann folgendermaßen ab:

- der Anfordernde identifiziert sich und die Information wird unverschlüsselt an das angeforderte Betriebssystem übermittelt;
- der Benutzer liest mit seiner Plastikkarte den dort gespeicherten, individuellen Chiffrierschlüssel in den Speicher des intelligenten Terminals ein; nur wenn dieser mit dem im Rechner unter seiner Identifikation gespeicherten übereinstimmt, ist ein weiterer Dialog möglich;⁸⁸
- der Rechner quittiert die (hier als korrekt angenommene) Identifikationsnachricht mit einer chiffrierten Aufforderung, ein Passwort einzugeben;
- der berechtigte Anwender gibt sein Passwort ein, und dieses wird - ebenso wie der gesamte folgende Dialog - verschlüsselt zur Überprüfung an den Rechner übertragen.

Dieses Verfahren hat einige bemerkenswerte Eigenschaften:

- der Chiffrierschlüssel, der selbstredend eine Authentifikations-Information darstellt, wird - im Gegensatz zu der Behauptung oben - niemals über den Datenkanal übertragen, kann also auch nicht abgefangen werden;
- da der Chiffrierschlüssel sowohl beim Benutzer als auch im System "bekannt" sein muß, ist der Schutz gegenseitig;
- das Passwort, das als zusätzlicher Schutz gegen Diebstahl der Plastikkarte erforderlich ist (s. nächsten Punkt), wird ausschließlich verschlüsselt übertragen;
- um erfolgreich ins System einzudringen, muß der "Feind" sowohl etwas an sich bringen, das der rechtmäßige Benutzer hat (die Plastikkarte), als auch etwas erfahren, das er weiß (das Passwort).

⁸⁶ Das Verfahren wird hier in der Darstellung von Saltzer und Schroeder [62] wiedergegeben.

⁸⁷ Dies ist mit dem rapide zunehmenden Einsatz von Arbeitsplatzsystemen keine wesentliche Einschränkung mehr.

⁸⁸ Bei Verbindungen zwischen Rechnern mit je einem eigenen Betriebssystem wird die Information auf der Plastikkarte durch eine ebensolche in der Benutzerliste des anfordernden Systems ersetzt; hierdurch wird die geforderte Symmetrie augenfällig erreicht.

Das Thema "Authentifikation" wurde an dieser Stelle recht ausführlich behandelt⁸⁹ nicht etwa, um sich in die Menge der erwähnten Veröffentlichungen einzureihen, sondern weil die Authentifikation eine entscheidende Rolle bei dem in Abschnitt 4 vorzustellenden, neuen Konzept des Verarbeitungsschutzes spielt.

3.4 Kontrollierte Mehrfachverwendung von Daten

Die Basis für jede Sicherheit im Sinne der Definition von Popek et al. zu Anfang des Abschnitts 3 ist die Möglichkeit, die Mitglieder einer "heterogenen Anwenderpopulation" gegenseitig total "abzuschotten", d.h. jedem einen disjunkten Daten- und Programmbereich zuzuweisen, und jede Art von Informationsfluß zwischen diesen zu verhindern, unabhängig davon, ob es sich um Daten oder Programme (als wirkende Subjekte) handelt. Dies ist trivialerweise dann möglich, wenn die Anwender jeweils in "reservierten Sitzungen" Alleinverfügungsrecht über das DV-System bekommen, und die Daten Dritter während dieser Zeit physikalisch abgetrennt werden.

Aber auch in einer Umgebung mit "Multiprogramming" - d.i. die Koexistenz vieler Benutzer bzw. deren Prozesse, die um die Systemdienste konkurrieren - ist die Aufgabe, eine gegenseitige Abschottung durchzuführen, im Prinzip relativ leicht. Es muß lediglich die Möglichkeit geschaffen werden, den Benutzern bzw. Benutzerkennungen ("principles"⁹⁰) je eigene, disjunkte Definitionsbereiche ("domains") zuzuteilen; diese bestehen aus den gespeicherten Datenbeständen (ggf. datenträgerbezogen) ebenso wie aus den Hauptspeicherbereichen, die ein aktiver Prozeß belegt. Obwohl die Organisation dieser unterschiedlichen Speicherkategorien bei vielen Betriebssystemen unterschiedlich gelöst wird, ist sie für die theoretische Darstellung von zweitrangiger Bedeutung und kann somit außer in konkreten Beispielen außer acht gelassen werden.

Die Abschottung der Definitionsbereiche ist eine Funktion der Systemarchitektur, die der Anwender als Software-schnittstelle zum DV-System erfährt. Bei der Analyse dieser Architektur ist es deshalb ebenfalls für die Zwecke dieser Ausführungen belanglos, welche Funktionen im realen Einzelfall durch Hard-, Soft- oder Firmware realisiert werden; ja es gibt nach außen kompatible Familien von DV-Systemen, in denen die einzelnen Mitglieder ein- und dieselbe Funktion unterschiedlich mit Hard-, Soft- oder Firmware bereitstellen.

⁸⁹ In der Tat stellt sie nur einen winzigen Ausschnitt der Gesamtdiskussion dar.

⁹⁰ Evans, Kantrowitz [17], Saltzer, Schroeder [62] - in etwa mit "Verantwortlichkeits-Träger" zu übersetzen.

Die bisher betrachtete gegenseitige "totale Abschottung" der Definitionsbereiche einzelner Anwender ist zwar Grundlage für den Datenschutz, genügt jedoch nicht den in der Praxis gestellten Forderungen. Vielmehr ist ein kontrollierter Austausch von Daten zwischen verschiedenen Anwendern oder eine gemeinsame Nutzung genau definierter Objekte erforderlich. Folgende Beispiele mögen dies verdeutlichen:

- die Mitarbeiter an einer Aufgabenstellung (z.B. Patientenaufnahme) oder einem Aufgabenkomplex (im selben Beispiel die Patientenverwaltung) müssen (pseudo-) gleichzeitig eine "Stammdatei" bearbeiten (hier die Patienten-Datenbank);
- tabellenartige Dateien (z.B. eine Kostenstellen-Datei) müssen global verfügbar sein;
- Dienstprogramme⁹¹ sollen ebenso wie Standard-Unterprogramme⁹² von allen Anwendern eingesetzt werden können.

Während das erste Beispiel offensichtlich keine Vervielfältigung der Daten in die einzelnen Definitionsbereiche zuläßt, da die vom einzelnen Anwender veranlaßte Änderung der Daten nur in einem gemeinsamen Bestand sinnvoll ist, könnte man sich naiv vorstellen, im 2. und 3. Fall vielfache Kopien der Datenbestände zu halten. Abgesehen von der offenkundigen, aber in vielen Fällen nicht ausschlaggebenden Verschwendung von Speicherplatz ergibt sich bei solchem Vorgehen ein in der Praxis unüberwindliches Problem mit Versionsänderungen und dergleichen. Es ist schon manches DV-Projekt daran gescheitert, daß disjunkte Datenbestände mit (teilweise) gleicher Bedeutung nicht konsistent gehalten werden konnten!

Das wirkliche Problem ist also nicht die Abschottung, sondern deren kontrollierte Überwindung (Mehrfachverwendbarkeit von Daten, "sharing"). Saltzer und Schroeder nennen dies das Hauptanliegen des Datenschutzes schlechthin ("key concern").

3.4.1 Grundtechniken

Um die Mehrfachverwendung von Daten zu realisieren, ist es erforderlich, ein Mittel bereitzustellen, das es erlaubt, die Sperren zu überwinden, die die Abschottung als grundlegender Schutzmechanismus darstellt. Dieses Mittel darf selbstredend nur einem - ggf. eingeschränkt - Zugriffsberechtigten zugänglich bzw. von ihm verwendbar sein. Es muß folglich neben dem technischen Vehikel der Überwindung eine damit untrennbar verbundene Information gegeben sein, die dessen Verwendung steuert.

Es gibt grundsätzlich zwei verschiedene Techniken, um die

⁹¹ Z.B. Compiler, Editoren, Listenerzeugungs-Programme usw.

⁹² Z.B. mathematische Funktionen oder die Realisierung installationsglobaler Konventionen.

gesteuerte Mehrfachverwendung zu verwirklichen, die den in Abschnitt 3.2 dargestellten Kategorien der ausweis- und listenorientierten Verfahren zuzuordnen sind. Die speziell für diesen Zweck geeigneten Ausweise werden "capabilities"⁹³ genannt; die listenorientierte Technik verwendet sogenannte "Zugriffs-Kontrolllisten" ("access control lists"⁹⁴). Diese beiden Mittel und ihre Anwendungsweise werden in den folgenden Unterabschnitten in Anlehnung an die Darstellung von Saltzer und Schroeder [62] vereinfacht dargestellt.

3.4.1.1 "Capabilities"

Unter einer "capability" ist ein spezielles Datenelement im Definitionsbereich des Anwenders zu verstehen, das in der Grundform aus zwei Teilen besteht:

- einer eindeutigen, unverwechselbaren Identifikation, die es dem Monitor ermöglicht, Lage und Umfang des geschützten Bereichs an Hand eigener, geschützter Informationen festzustellen⁹⁵ und
- einer Aufzählung der mit dieser "capability" zugestandenen Befugnisse.⁹⁶

Ohne eine entsprechende "capability" zu besitzen, kann kein Benutzer in einem auf dieser Basis organisierten System auf die zugeordneten Daten zugreifen - auch nicht auf die eigenen. Der Besitz einer "capability" dagegen wird als "prima facie"-Beweis dafür gewertet, daß ein Subjekt die darin dokumentierten Zugriffsrechte besitzt.⁹⁷ Der Zugriff auf ein Objekt geht so vor sich, daß das Subjekt dem Adressierungsmechanismus (dem Monitor) die zugehörige "capability" übergibt - i. allg. zusammen mit einem Wert, der den Abstand des gewünschten Datenfelds vom Objektanfang angibt. Aus beiden Werten kann der Monitor das Objekt auffinden und prüfen, ob der angegebene Abstand seine Grenzen nicht überschreitet - also keine Daten bezeichnet, deren Zugriff nicht durch diese "capability" erlaubt ist.

"Capabilities" haben die bei Ausweisen sonst nicht übliche

⁹³ Dennis, Van Horn [11]; das Wort "capability" läßt sich in etwa mit "(Zugriffs-)Befähigung" übersetzen; in diesem Zusammenhang sind jedoch datenähnliche Gebilde gemeint, die als "Träger" dieser Befähigung dienen. Da weder die wörtliche Übertragung den vollen Inhalt wiedergibt, noch ein treffender deutscher Ausdruck gefunden wurde, soll in diesem Fall der englische Begriff beibehalten, aber stets in Anführungszeichen gesetzt werden.

⁹⁴ Saltzer [61].

⁹⁵ Man beachte, daß es sich hier gerade nicht um explizite Adressierungs-Informationen handelt.

⁹⁶ Der Besitz einer "capability" stellt im Sinne des Abschnitts 3.2 bereits eine implizite Zugriffsbefugnis-Information dar, die jedoch nach dem Grundprinzip der Minimalbefugnisse explizit erweitert werden muß, wenn weitergehende Funktionen an den Daten erfolgen sollen.

⁹⁷ Lampson [40].

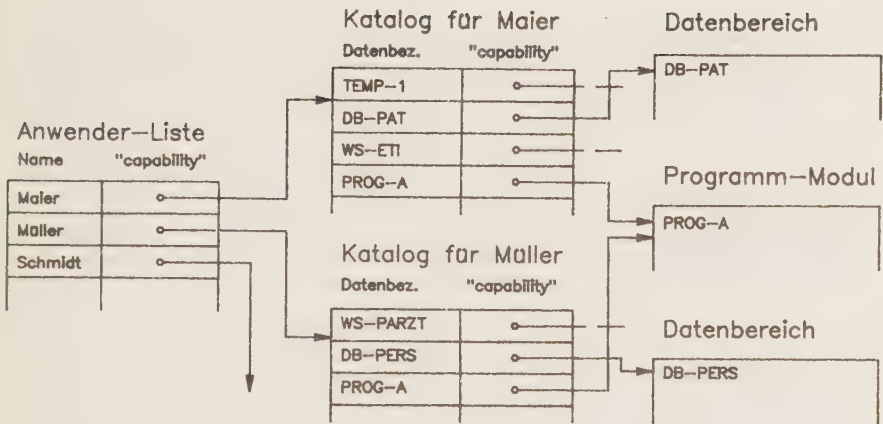


Abb. 3: Zugriff auf Speicherbereiche mit Hilfe von "capabilities"

Eigenschaft, daß sie vervielfältigt und weitergegeben werden dürfen; hierauf beruht geradezu die Mehrfachbenutzbarkeit der beschriebenen Objekte. Da aber Ausweise weder gefälscht noch verfälscht werden dürfen,⁹⁸ ist es notwendig, sie streng von den anderen Daten zu unterscheiden: das System muß entweder je Datenelement eine Anzeige ("tag bit") reservieren, das die "capability"-Eigenschaft kennzeichnet, oder es muß disjunkte Speicherbereiche unterscheiden, die entweder ausschließlich "gewöhnliche" Daten oder nur "capabilities" enthalten können. Dann kann es sicherstellen, daß "capabilities" nicht beliebig, sondern nur mit einem eigenen, eingeschränkten Befehlssatz verarbeitet werden können, der im wesentlichen aus Kommandos besteht

- zum Kopieren der "capabilities" und
- zur Veränderung der Zugriffs-Befugnisse - sofern die Befugnis hierzu vorliegt.

Unstatthaft dagegen ist nach dem bisher Gesagten jede Veränderung des Bitmusters, das das zugehörige Objekt dem Monitor gegenüber identifiziert.

Da Prozesse i. allg. mehrere Objekte benutzen (mindestens den Bereich der aktiven Prozedur und deren Datenbereich), besitzen sie generell eine Vielzahl von "capabilities";⁹⁹ die hierarchisch gegliedert und über die zugreifbaren Objekte verteilt sein kann. Bei der Initialisierung eines

⁹⁸ Verfälschung heißt bei "capabilities" in erster Linie, daß ihre Identifikation abgeändert wird, um auf ein anderes Objekt zu weisen.

⁹⁹ Diese Menge wird in der Literatur manchmal als "C-Liste" bezeichnet.

Prozesses erhält dieser zunächst eine "capability" für seinen "Katalog" (Abb. 3), der die erste hierarchische Ebene seiner Zugriffsberechtigungen - die "capabilities" seiner "Basis-Objekte" - enthält, und von dem aus weitere "capabilities" erreichbar sein können.

Um aber zu einer Mehrfachverwendung von Objekten zu gelangen, muß es im Betriebssystem zusätzlich einen Kanal geben, der es dem Besitzer einer "capability" ermöglicht, diese an einen anderen Anwender - ggf. mit geänderten Befugnissen¹⁰⁰ - zu "senden", und letzterem, sie zu "empfangen", wodurch das beschriebene Objekt für ihn im Rahmen der übertragenen Befugnisse zugreifbar wird.

So einfach dieses Prinzip klingt, so schwerwiegende Probleme wirft es auf. Diese betreffen in erster Linie die "Dynamik" der Mehrfachverwendbarkeit, d.i. das Verhalten bei Löschung eines Objekts, Veränderung seiner Eigenschaften oder Rücknahme einer erteilten Zugriffsberechtigung, in den letzten Fällen vor allem, wenn diese Maßnahme nicht alle Anwender betrifft, denen zuvor eine Berechtigung zugestanden wurde. Der Besitzer ist i.allg. nicht in der Lage, eine einmal weitergereichte "capability" zu löschen oder zu ändern, da sie sich ja nun im Definitionsbereich des Empfängers befindet, und somit für ihn meist nicht zugreifbar ist; ja, er hat generell keine Möglichkeit, auch nur die Lage der "capability" im Definitionsbereich des Empfängers festzustellen!¹⁰¹ Aber auch wenn ihm dies alles ermöglicht würde, oder er den Empfänger auf irgend eine Weise zwingen könnte, die Änderung selbst durchzuführen, ist er selbst gezwungen, streng buchzuführen, um alle Kopien wiederaufzufinden. Verschlimmert wird die Situation erheblich, wenn der Empfänger die "capability" seinerseits kopieren oder gar an Dritte weiterreichen kann; deshalb beschränken manche Systeme, die den Zugriff zu Daten mit "capabilities" organisieren, deren Weitergabe mit Hilfe einer weiteren - vom Anwender nicht beeinflussbaren - Anzeige auf einen Vorgang: eine Kopie einer "capability" kann ihrerseits nicht kopiert werden. Eine andere Lösung dieser Schwierigkeit besteht darin, ausschließlich "indirekte capabilities" weiterzureichen, das sind solche, deren Objekte die eigentlichen "capabilities" für die mehrfach zu verwendenden Objekte sind: durch das Löschen der primären "capability" werden alle indirekten einschließlich ggf. angefertigter Kopien wirkungslos. Eine solche indirekte Zugriffstechnik ist allerdings mit hohen Effizienzverlusten behaftet.

Trotz aller Probleme ist die kontrollierte Überwindung der Abschottung mit Hilfe von "capabilities" in seiner Grundform sehr effizient, und es gibt deshalb eine umfangreiche

¹⁰⁰ Für gewöhnlich wird wenigstens die Befugnis, Zugriffsbefugnisse zu ändern, nicht weitergegeben.

¹⁰¹ Man beachte die Analogie zu den in Abschnitt 2.1.1 angeführten Befürchtungen in bezug auf den Verlust der Kontrolle über einmal an Dritte übermittelte Daten.

Literatur, die sich mit diversen Ausprägungen der grundsätzlichen Technik befaßt, und Lösungswege für die damit verbundenen, vielfältigen Probleme aufzeigt. Neben den bereits angegebenen Stellen sind u.a. noch Fabry [18], Linden [44], Popek und Kline [52] sowie Wulf et al. [82] zu nennen.

Es muß ausdrücklich darauf hingewiesen werden, daß Datei-Kennwörter - trotz ihrer Ausweisfunktion - keine "capabilities" sind; denn sie beinhalten keine Information, die es einem Monitor ermöglichen könnte, die geschützten Daten zu lokalisieren; ja es können verschiedene Datenbestände mit identischen Kennwörtern geschützt sein. Die Kenntnis eines Kennworts zu einem Objekt ist wirkungslos, wenn der Zugriff - z.B. in Ermangelung der zugehörigen, echten "capability" - selbst verwehrt ist. In der bisher gebräuchlichen Verwendungsweise stellen Datei-Kennwörter deshalb lediglich eine "zweite Verteidigungslinie" dar, um einen Mißbrauch der Daten zu verhindern, auch wenn der Zugriffsmechanismus selbst kompromittiert wurde - z.B. indem ein "Einbruch" in eine fremde Kennung gelingt (Versagen des Benutzungsschutzes) oder eine "capability" unzulässig weitergegeben wurde.¹⁰²

3.4.1.2 Zugriffs-Kontrolllisten

Eine Zugriffs-Kontrollliste ist eine Datenstruktur, die aus mindestens zwei unterschiedlichen Elementen besteht:

- der Adressierungs-Information für die beschriebene Datenmenge und
- einer Aufzählung aller zugriffsberechtigten Subjekte/erreichbaren Objekte mit zugehörigen Befugnissen.

In einer Umgebung, die Zugriffs-Kontrolllisten einsetzt, um Objekte vor unberechtigtem Zugriff zu schützen, muß das Betriebssystem für jedes neu erzeugte Objekt auch eine neue Kontrollliste erstellen, wobei standardmäßig dem Erzeuger (Besitzer) alle Zugriffsrechte - einschließlich dem Recht, diese zu verändern - zugesprochen werden, allen anderen Benutzern dagegen keine.

Zugriffs-Kontrolllisten können in einem systemweit gültigen "Katalog" zusammengefaßt werden; es können aber auch Katalog-Hierarchien gebildet werden.¹⁰³ Der Aufbau eines solchen

¹⁰² Bei der Verwendung von Datei-Kennwörtern kann allgemein eine Potenzierung der Probleme festgestellt werden, die von Passwörtern her bekannt sind, da die Anzahl zu schützender Dateien größer ist, als die der Anwender, und da ferner oft mehrere Anwender das Kennwort einer Datei benötigen. Deshalb sind Datei-Kennwörter auch schwerer zu ändern. Erst durch die in Abschnitt 4.4 darzustellende Technik zur Realisierung des Verarbeitungsschutzes erhalten sie eine neue, mächtigere Wirkung.

¹⁰³ Dann stellt die Liste der zugelassenen Benutzerkennungen einen Katalog zur ersten, benutzerspezifischen Katalog-Ebene dar.

Katalog		
. . .		
DAT-PAT	zugelassene Benutzer	
Adresse	Maier	lesen/verändern
PROG-A	zugelassene Benutzer	
Adresse	Maier	ausfahren
	Müller	ausfahren
DAT-PERS	zugelassene Benutzer	
Adresse	Müller	lesen/anfragen
. . .		

Abb. 4: Zugriffs-Kontrollliste

Katalogs ist in Abb. 4 dargestellt. Im Gegensatz zu den "capabilities" können Zugriffs-Kontrolllisten - zumindest die, die sich im hierarchisch höchsten Katalog befinden - mit Hilfe des Datei-Namens von allen Benutzern angesprochen werden. Der Zugriff zu dem beschriebenen Objekt wird aber vom Monitor nur dann gestattet, wenn dies dem anfordernden Subjekt mit den zur gewünschten Zugriffsart passenden Befugnissen explizit erlaubt ist. Während der Besitz einer (Kopie einer) "capability" bereits Zugriffsrechte zum zugeordneten Subjekt impliziert, dienen die (je Objekt einmalig vorhandenen) Zugriffs-Kontrolllisten dazu, festzustellen, ob solche Rechte bestehen. Durch die eindeutige Beziehung zwischen Objekt und Kontrollliste werden die bei der Beschreibung der "capabilities" angedeuteten Probleme mit der Dynamik der Datenbestände vermieden.

Zugriffs-Kontrolllisten können einen erheblichen Komplexitätsgrad erreichen, wenn eine Vielzahl unterschiedlicher Subjekte mit je verschiedenen Befugnissen Zugriffsrechte bekommen sollen. Ihre Verwendung ist deshalb weniger effektiv als die der "capabilities"; dieser Nachteil kann durch die bereits in Abschnitt 3.2 beschriebene Maßnahme gemildert werden: nach positiv verlaufener Berechtigungsprüfung an Hand der Zugriffs-Kontrollliste wird - für den Anwender "unsichtbar" - eine "transiente" (d.h. kurzlebige, spätestens mit dem Prozeßende ungültig werdende) "capability"

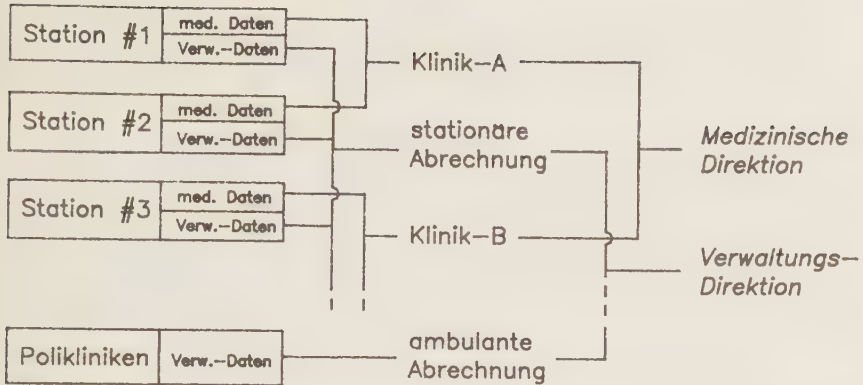


Abb. 5: Gruppen-Struktur (Beispiel)

vom Monitor aus der Liste erzeugt und sichergestellt; diese wird fortan zum beschleunigten Zugriff herangezogen. Es wird also mit Hilfe eines temporären Ausweises ein "Mischsystem" erzeugt. Da die Zugriffsberechtigung aber nur noch beim ersten Zugriff geprüft wird, reduziert sich die Möglichkeit dynamischer Veränderungen geringfügig; Änderungen an bereits im Zugriff befindlichen Objekten werden erst nach Beendigung der laufenden Prozesse oder bestenfalls der aktiven Prozeduren für die betreffenden Subjekte wirksam.

Es ist offensichtlich, daß sich der Einsatz von Zugriffs-Kontrolllisten wegen ihrer komplexeren Struktur und Funktion vorzugsweise dann eignet, wenn es gelingt, die Listen selbst kurz zu halten. Eine weit verbreitete Methode hierzu ist die Bildung von Benutzergruppen, deren Mitglieder alle dieselben Befugnisse besitzen. Solche Gruppen lassen sich ebenfalls hierarchisch gliedern, wobei dann die Befugnisse einer Ebene eine Untermenge der nächsten sind. Diese Einteilung reduziert nicht nur die Länge der Listen erheblich, sie entspricht auch häufig anzutreffenden Organisationsformen der Nutzer-Populationen. In einem Klinikum etwa kann man verschiedene Arbeitsgebiete unterscheiden und hierarchisch strukturieren, wie Abb. 5 zeigt.¹⁰⁴ Selbstverständlich kann dieses einfache Beispiel beliebig erweitert und verfeinert werden, indem etwa

- neue Ebenen eingezogen werden; so könnten beispielsweise
 - je Klinik - unter Erweiterung der poliklinischen Daten ein stationärer und ambulanter Bereich unterschieden werden,
 - unter der Verwaltungsdirektion zwischen allgemeiner Patientenabrechnung, Lagerverwaltung, Rechnungswesen usw. unterschieden werden;

¹⁰⁴ S. auch beispielsweise Klar, Pietrzyk [37].

- zentrale Leistungsstellen, wie die Apotheke, ein klinisch-chemisches Labor oder eine Röntgenabteilung Zugriff zu Teilen der Stationsdaten erhalten und umgekehrt.

Wesentlich ist, daß eine übergeordnete Angabe (wie etwa Klinik-A) in einer Zugriffs-Kontrollliste die explizite Nennung der zugehörigen Benutzerkennungen (hier die der Stationen #1 und #2) erspart. Hinzu kommt eine erweiterte dynamische Wirksamkeit: beispielsweise braucht die Abgabe der Station #2 an Klinik-B oder die Hinzunahme einer Station #4 lediglich in der Gruppendifinition eingetragen zu werden, nicht jedoch in den betroffenen Zugriffs-Kontrolllisten unbestimmter Anzahl. Als Kurzbezeichnung für eine definierte Benutzermenge stellt eine Gruppe somit ein "Über-Subjekt" dar.

Für die Realisierung der Gruppenstrukturen, d.h. den Mechanismus, mit dem vom Benutzer auf die Gruppe geschlossen wird und/oder umgekehrt, gibt es mehrere Verfahren, auf die an dieser Stelle nicht eingegangen werden kann!⁰⁵ Man beachte jedoch, daß man durch Bildung einer hierarchisch äußeren Globalgruppe, die sämtliche Benutzer enthält, das in Abschnitt 3.2 geforderte spezielle Listenelement "Alle" zwanglos einführen kann!⁰⁶

3.4.2 Zugriffs-Matrix, Objektschutz

In den bisherigen Erörterungen zur kontrollierten Mehrfachverwendung wurden die Begriffe "Subjekt" und "Objekt" ohne nähere Definition verwendet. In manchen Zusammenhängen wurden auch die Begriffe Anwender oder Benutzer(kennung) einerseits, sowie Datei oder Datenbestand andererseits, jeweils quasi-synonym hierzu eingesetzt, um die Zusammenhänge konkreter darstellen zu können, und dies entspricht auch weitgehend der DV-technischen Praxis: der Anwender - bzw. stellvertretend seine Benutzerkennung - wird als wirkendes

¹⁰⁵ Ebenso kann an dieser Stelle nur angedeutet werden, daß es unterschiedliche "Gruppen-Philosophien" gibt: in manchen Systemen dient die Hierarchisierung zur Überwachung und Steuerung durch vorgeordnete Anwender (Vorgesetzte); in anderen wird die umfassendere Schicht verwendet, um Datenbestände, Methoden usw. bereitzustellen, die den Gruppenmitgliedern gemeinsam verfügbar sein sollen (Stammdaten und dergl.). Diese beiden Extreme können mit relativ einfachen technischen Mitteln realisiert werden, weil jeweils nur eine Schlußrichtung (Gruppe → Anwender bzw. Anwender → Gruppe) verwirklicht werden muß; ein Mittelweg, der beide Schlußfolgerungen erlaubt, erfordert dagegen beträchtlich höheren Aufwand.

¹⁰⁶ Im Extremfall, daß neben den individuellen Benutzern nur noch eine Globalgruppe vorgesehen ist (jeder Datenbestand ist entweder nur dem Besitzer oder der ganzen Benutzerpopulation zugänglich), reduziert sich die Kontrollliste auf eine einzige Anzeige. Systeme dieser Art bezeichnen Saltzer und Schroeder [62] als "all or nothing"-Systeme, und sie zählen sie gar nicht zu den gesicherten.

Subjekt betrachtet, das je Datenbestand ein - ggf. qualifiziertes - Recht auf Zugriff hat oder nicht. Es wird also ein einfacher, zweidimensionaler Zusammenhang gebildet, der die Befugnisse eines jeden Anwenders gegenüber jedem Datenbestand definiert.

In einer umfassenderen Darstellung genügt diese Einschränkung der Subjekteigenschaft jedoch nicht. Bei differenzierterer Betrachtungsweise ergibt sich nämlich die Notwendigkeit, auch zeitlich begrenzte Funktionen wie Prozesse oder aktuell ablaufende Prozeduren als wirkende Subjekte anzusehen, die die Befugnisse der veranlassenden Anwender übernehmen oder auch temporär einschränken bzw. durch eigene Rechte erweitern können. Da solche Subjekte jedoch von anderen beeinflußt werden können (Anwender starten und beenden Prozesse, Prozesse können den Ablauf anderer steuern

		O B J E K T E							
		Subjekte				Dateien/Datenträger			
		S ₁	S ₂	...	S _n	D ₁	D ₂	...	D _k
S U B J E K T E	S ₁		anhalten			lesen zufügen			ausführen
	S ₂				beenden		lesen		"Besitzer" verändern
	.								
	.								
	S _n	wieder- starten					löschen	erweitern	

Abb. 6: Zugriffs-Matrix

usw.), ergibt sich, daß sie auch als Objekte betrachtet werden müssen!¹⁰⁷

Die ersten Bemühungen, die Probleme der Mehrfachverwendung zu formalisieren, gingen deshalb von einer zweidimensionalen "Zugriffs-Matrix" ("access matrix"¹⁰⁸) aus, bei der die wirkenden Subjekte zusätzlich als Objekte erscheinen (Abb. 6). Graham und Denning [22], Schulze [66], sowie Turn und

¹⁰⁷ In einer Betriebssystemumgebung, die das Recht, Benutzerkennungen zu erzeugen, zu sperren, aufzuheben und ihnen Befugnisse zu erteilen, nicht dem Systemverwalter vorbehält, sondern an delegierbare Befugnisse knüpft, gilt diese Subjekt/Objekt-Ambivalenz auch für die Kennungen.

¹⁰⁸ Martin [46] benutzt für die entsprechende Struktur den Begriff "authorization scheme".

Ware [76] schildern ausführlich Varianten eines Sicherheitskonzepts auf dieser Basis,¹⁰⁹ wobei die Subjekte stets durch Zeilen, die Objekte durch Spalten dargestellt werden.

Auch bei den Objekten ist eine Begriffsausweitung erforderlich, um die durch die Zugriffs-Matrix dargestellten Beziehungen zu vervollständigen: neben den primären Datenbeständen, die in Dateien oder auf eigenen Datenträgern residieren, sind auch Datenkanäle, wie sie Interprozeß- und Interprozessor-Kommunikation, mehrfachverwendbare oder systemglobale Variable oder Signale usw. darstellen, durch Subjekte zu beeinflussen. Oft - vor allem wenn große Datenbanken geschützt werden müssen - ist es ferner notwendig, einzelne *Datenfelder* - das sind definierte Teilbereiche eines Datenbestands - als selbständige Objekte zu betrachten. Man erkennt, daß der Verfeinerungsgrad der Betrachtungsweise vom Standpunkt und Aussageziel dessen abhängt, der ein Sicherheitssystem beschreibt oder entwirft. Es muß nochmals betont werden, daß die Anwenderschnittstellen fast aller verbreiteten Betriebssysteme ausschließlich Benutzerkennungen als Subjekte erkennen, und auch bei den Objekten nicht alle der angeführten Möglichkeiten berücksichtigen!¹¹⁰

An den Schnittstellen der Zeilen und Spalten der Zugriffs-Matrix werden die Berechtigungen (falls vorhanden) eingetragen, die das betreffende Subjekt dem bezeichneten Objekt gegenüber besitzt. Hierzu gehören Befugnisse, wie sie in Abschnitt 2.3.2.4 differenziert wurden, die diversen Möglichkeiten der Subjekte, sich gegenseitig zu beeinflussen, aber auch weitergehende Eigenschaften und damit verbundene Befugnisse, wie beispielsweise "Besitzer" mit dem Recht des Subjekts, die Zugriffsberechtigungen zum bezeichneten Objekt (d.h. alle Eintragungen in eben dieser Spalte) festzulegen oder zu verändern. Ferner wird manchmal die Möglichkeit gefordert, bedingte Berechtigungen vorzusehen, sei es, daß äußere Umstände - wie etwa die Uhrzeit - die aktuellen Befugnisse bestimmen, sei es, daß sie vom Zustand anderer Objekte abhängig gemacht werden. Selbstredend erhöhen solche Variationen die darstellerische und funktionale Komplexität erheblich und können beträchtliche Probleme dynamischer Art aufwerfen.

Die Zugriffs-Matrix darf nur als Denkmodell oder "abstrakter Sicherheitszustand" ("protection state"¹¹¹) des Systems aufgefaßt werden;¹¹² in der Praxis ist sie - als Datenobjekt - ungekürzt nicht handhabbar. Ein Versuch, sie, wie beschrieben, physikalisch zu verwirklichen, würde bereits bei kleinen Systemen in riesige Dimensionen führen; dabei dürften wegen des Grundprinzips der standardmäßigen Zugriffs-

¹⁰⁹ S. auch Conway et al. [7], Harrison, Ruzzo [29], Hoffman [31], Rüdel [60].

¹¹⁰ Linden [44].

¹¹¹ Graham, Denning [22].

¹¹² Hierfür ist sie allerdings sehr gut geeignet; s. z.B. die Ausführungen von Harrison, Ruzzo [29] zur Entscheidbarkeit.

verweigerung weitaus die meisten Schnittstellen-Felder leer sein ("sparse matrix"). Aber auch die Dynamik eines solchen Gebildes wäre wohl kaum zu bewältigen: mit jedem neuen Objekt muß eine vollständige, neue Spalte hinzugefügt werden, und für ein neues Subjekt gar sowohl eine Zeile als auch eine Spalte. Diese Probleme potenzieren sich mit der Verfeinerung der Subjekteigenschaft in den funktionalen Bereich, da dann ein wesentlicher Teil der Dynamik des Gesamtsystems abgebildet werden muß. Ein solcher Aufwand zur Darstellung einer weitgehend leeren Datenstruktur¹¹³ verbietet sich von selbst; für eine praktische Realisierung des Sicherheitsprinzips ist eine strukturelle Vereinfachung geboten.

Nach dem bisher Gesagten ist es naheliegend, die Zugriffsmatrix durch Elimination der leeren Elemente zu reduzieren. Durch diese Maßnahme wird aber - je nach Betrachtungsweise - die Zeilen- oder Spalten-Struktur der Matrix aufgelöst; es wird erforderlich, den Elementen eine Bezugsinformation beizugeben.

Turn und Ware [76] beschreiben ausführlich eine Zerlegung der Zugriffsmatrix in eine Vielzahl von Listen, die den um die leeren Elemente gekürzten Zeilen oder Spalten entsprechen. Dies ist offensichtlich die theoretische Basis der bereits erläuterten, listenorientierten Schutzmechanismen. Eine weitere Vereinfachung führt Hoffman [31] ein, indem er stets identische Listeneinträge zusammenfaßt; hierdurch werden die bereits erläuterten Gruppenbildungen untermauert. Ein anderer Weg, die bereits reduzierte Matrix weiter zu vereinfachen, besteht darin, die verbleibenden Schnittstellen-Felder nicht zu Listen zusammenzutragen, sondern als Einzelgebilde zu betrachten, die je die Befugnisse eines (besitzenden) Subjekts einem definierten Objekt gegenüber angeben. Offensichtlich handelt es sich bei diesen Elementarangaben um Ausweise. Es ist diese Ausweiskfunktion der gesondert betrachteten Matrixelemente, die eine feste Zuordnung zu den Subjekten erforderlich macht; obwohl keine solche funktionale Notwendigkeit bei Listen vorliegt, werden diese - mit einer Ausnahme¹¹⁴ - stets den Objekten zugeordnet.

Der Unterschied zwischen den ausweis- und listenorientierten Techniken zur kontrollierten Mehrfachverwendung von Daten ist darin zu erkennen, daß Listen stets *vollständige*, wenn auch um die leeren Elemente gekürzte Spalten oder Zeilen der Zugriffsmatrix darstellen; der Ausweis dagegen ist ein Einzelelement: die Menge der aktuell von einem Subjekt vorgewiesenen Ausweise stellt eine *unvollständige*

¹¹³ Selbstredend stellen leere Elemente der Zugriffsmatrix ebenfalls Informationen dar, nämlich die, daß das betreffende Subjekt *keine* Rechte über das bezeichnete Objekt besitzt; ihr Beitrag zur Entropie der Gesamtmatrix ist jedoch verschwindend.

¹¹⁴ Young [83].

Zeile dar!¹⁵ Es ist diese Unvollständigkeit der aktuell eingesetzten Matrix-Zeile, die die ausweisorientierten Schutzmechanismen effizienter macht; der Umgang mit Einzelinformationen erleichtert deren Weitergabe, erzeugt aber auch die bereits dargestellten dynamischen Probleme.

Alle Verfahren, die sich letztendlich allein auf die Zugriffs-Matrix zurückführen lassen, schützen Objekte unabhängig von ihrem Inhalt und dessen "Wert". Rüdel [60] bezeichnet solche Methoden deshalb treffend mit dem Begriff "Objektschutz". Im folgenden Abschnitt wird zu zeigen sein, daß diese Techniken allein beim Umgang mit sensitiven Daten nicht ausreichen. Da aber die Mehrzahl der Autoren, die weiterführende Verfahren beschreiben – wohl der darstellerischen Klarheit wegen – einen Gegensatz zwischen diesen und dem Objektschutz implizieren, ist es wichtig, festzustellen, daß jene vielmehr nur auf der Basis eines funktionierenden Objektschutzes im Sinne einer Erweiterung oder Ergänzung sinnvoll sind.

3.4.3 Vertrauensaspekte

Die wesentliche Schwäche des reinen Objektschutzes ist darin zu suchen, daß Eigenschaften wie Vertraulichkeit und Vertrauen bzw. Vertrauensmangel unberücksichtigt bleiben. Zweifel an der Vertrauenswürdigkeit können sich sowohl auf den menschlichen Umgang mit Daten beziehen als auch auf die – selbstredend von Menschen erstellten – Verfahren. Zum Schutz gegen menschliche Vertrauensbrüche ist ein Sicherheitskonzept entwickelt worden, das Rüdel [60] mit "Informationsschutz" bezeichnet; gegen verdächtige Verfahren schützen mehrere Techniken, die das Prinzip der Minimalbefugnisse in der Prozedurebene zu realisieren trachten.

3.4.3.1 Informationsschutz

Im Rahmen des Objektschutzes ist es dem Anwender freigestellt, wie er innerhalb seiner Befugnisse mit den verfügbaren Daten umgeht; die Maßnahmen zum Objektschutz werden deshalb in der Literatur häufig als "discretionary sharing" (sinngemäß: "Mehrfachverwendung mit freiem Ermessensspielraum über die Ausnutzung der Zugriffsrechte") genannt. Es tritt aber erfahrungsgemäß häufig der Fall auf, daß dem zugriffsberechtigten Subjekt – vor allem in bezug auf die Weitergabe von Daten – Schranken gesetzt werden müssen; denn in vielen Anwendungen gibt es Daten mit verschiedenen

¹⁵ Um diese Unvollständigkeit zu verdeutlichen, sei das Beispiel des Kongreßteilnehmers aus Abschnitt 3.2 ein wenig weitergeführt: der dort angeführte Saalordner interessiert sich ebensowenig für die Fahrkarte, die den Teilnehmer berechtigt, zum Kongreßort zu reisen, wie etwa der Zugschaffner für den dort Einlaß gewährenden Namens-Anstecker; ein Subjekt ist offensichtlich in der Lage, aktuell benötigte Befugnisse nach Bedarf getrennt einzusetzen.

Geheimhaltungsanforderungen!¹⁶ Dementsprechend lassen sich die Anwender (Subjekte) in verschiedene Vertrauensstufen einordnen, und es muß verhindert werden, daß eine Vertrauensperson ihr zugängliche Informationen verrät, etwa indem sie sie in eine Datei niedrigerer Vertraulichkeit überträgt, die geringeren Kontrollen unterworfen ist!¹⁷ Ähnliches gilt in bezug auf die "Arbeitsbereiche", die sich in einem komplexen System unterscheiden lassen!¹⁸ Diese sollten nicht mit den hierarchischen Gruppenstrukturen, wie sie zur Vereinfachung der Objektschutzmechanismen eingeführt wurden, verwechselt werden, obwohl sie intern durchaus mit solchen Mitteln gegliedert werden können. Es handelt sich hierbei vielmehr um blockartige, disjunkte Daten- und Verarbeitungsbereiche; ein Informationsaustausch zwischen diesen "Kategorien" ist jedem Benutzer möglich, der beiden angehört; dies gilt natürlich im Rahmen seiner Zugriffsrechte in den einzelnen Kategorien und seiner Vertrauensstufe; generell wird aber der streng hierarchische Aufbau der Gruppen nicht verlangt.

Es besteht also ein Bedarf, *technische* Mittel bereitzustellen, die der Mehrfachverwendung von Daten Grenzen setzen, welche auch von einem zugriffsberechtigten Benutzer nicht überschritten werden können. Man spricht dann von "indiscretionary sharing" ("Mehrfachverwendung, die dem Ermessen des Anwenders nicht unterworfen ist"). Mit diesem Ziel hat Bell ein "Klassifikations-prinzip" entwickelt, das diesen Forderungen gerecht wird, und von Rüdel [60] "Informationsschutz" genannt wird. Walter et al. [79] haben theoretische Modelle hierzu entwickelt, und Denning [8] formalisiert die zugehörigen Prüfbedingungen; Millen [48] und Popek et al. [54] beschreiben Beweistechniken auf dieser Basis!¹⁹ Sehr ausführlich wird die Methodik im Rahmen der Entwicklung einer verallgemeinerten "Sicherheits-Philosophie" von Young [83] beschrieben; die nachstehende Erläuterung folgt weitgehend seiner Darstellung.

Die Struktur eines Informationsschutz-Systems wird fast durchweg als ein Gitter ("lattice") dargestellt, bei dem die disjunkten Kategorien oder Arbeitsbereiche durch senkrechte Linien dargestellt werden, und die Höhe der waage-

¹¹⁶ Z.B. "streng geheim", "geheim", "vertraulich", "allgemein verwendbar" oder auch "VIP-Patienten-Daten" (die gegenüber der Boulevardpresse u. dergl. ein erhöhtes Schutzbedürfnis haben), "Patienten-Daten", "anonymisierte Patienten-Daten", "nicht personenbezogene Daten".

¹¹⁷ Dies wäre zwar ein Vertrauensbruch, der jedoch im angesprochenen, menschlichen Bereich nicht auszuschließen, ja, oft mit katastrophalen Folgen vorgekommen ist (Fuchs' Verrat der Geheimnisse der Atom-bombenherstellung!); s. hierzu die Anmerkungen in Abschnitt 1 über die Vorteile technischer gegenüber organisatorischer Schutzmaßnahmen.

¹¹⁸ Z.B. "Medizin", "Patienten-Verwaltung", "Personal-Verwaltung", "Rechnungswesen", "Institut XYZ", "Forschungsbereich ABC" usw.

¹¹⁹ S. Fußnote 58.

rechten Zeilen das Vertraulichkeitsmaß der Daten bzw. Anwender versinnbildlicht (Abb. 7). Diese Einteilung liegt auch der Sicherheits-Philosophie von Young zugrunde, die jedes Subjekt und jedes Objekt mit einem eigenen "Sicherheits-Niveau" versieht. Diese besteht aus einem Elementepaar:

- Das erste Element heißt bei Objekten die "Geheimhaltungsstufe" und deren mögliche Werte sind eindeutig geordnet,¹²⁰ so daß der Operator " $\geq$ "¹²¹ definiert ist; sie entsprechen der Höhe der waagerechten Linien im Gitter. Bei Subjekten wird dieses erste Element "Vertrauenswürdigkeit" genannt und kann Werte aus demselben Definitionsbereich annehmen. In Anlehnung an den englischen Sprachgebrauch nennt man eine solche Einteilung "Klassifizierung"; Daten, die nicht vertraulich sind, heißen "unklassifiziert".

		K A T E G O R I E N			
		Bereich 1	Bereich 2	Bereich 3	
V E R T R A U L I G K E I T	Streng geheim				
	Geheim				
	Vertraulich				
	Frei zugänglich				

Abb. 7: Informationsschutz-Gitter

- Das zweite Element des Sicherheits-Niveaus ist eine Menge von disjunkten "Kategorien",¹²² die, wie bereits erläutert Arbeitsbereiche, abgeschlossene Wissensgebiete o.ä. darstellen können. Ein Sonderfall ist die sogenannte Φ -Kategorie; auf Objekte bezogen kennzeichnet sie solche, die allgemein verfügbar sind ("public")¹²³ und entspricht dem "Alle"-Element bei den listenorientierten Schutztechniken;¹²⁴ bei Subjekten ist die Φ -Kategorie stets implizites Element der zugeordneten Kategorie-Menge; somit ist gewährleistet, daß jedes Subjekt - auch eines mit explizit leerer Kategorie-Menge - auf solche "public"-Objekte zugreifen kann - letzteres allerdings auch nur auf diese.

¹²⁰ S. Fußnote 116; selbstverständlich können auch nur zwei Stufen ("schützen"/"verfügbar") oder auch beliebig viele definiert werden.

¹²¹ Zu lesen: "größer oder gleich".

¹²² Es können folglich sowohl Objekte als auch Subjekte mehreren Kategorien angehören.

¹²³ Nicht zu verwechseln mit dem auf Direktzugriffs-Datenträger angewandten "public"-Begriff!

¹²⁴ S. Abschnitte 3.2 und 3.4.1.2

Um nun Sicherheits-Niveaus miteinander vergleichen zu können (d.h. um eine Zugriffsberechtigung zu überprüfen), führt Bell einen Operator "dominiert" ein:

das Sicherheits-Niveau A dominiert das Sicherheits-Niveau B, wenn gilt:

Geheimhaltungsstufe/}
Vertrauenswürdigkeit} von A $\geq$ Geheimhaltungsstufe von B

und

Kategoriemenge von A $\supseteq$ Kategoriemenge von B.¹²⁵

Mit diesen Definitionen werden 6 Bedingungen von Young postuliert, die ein sicheres System kennzeichnen sollen; für die aktuelle Betrachtung sind folgende drei von Interesse!¹²⁶

- Ein Subjekt darf nur dann auf ein Objekt zugreifen, wenn sein Sicherheits-Niveau das des Objekts dominiert (einfache Sicherheitsbedingung).
- Ein Subjekt darf ein Objekt A nur dann in Abhängigkeit von einem Objekt B verändern, wenn das Sicherheits-Niveau von A das von B dominiert ("*-Bedingung", "*-Eigenschaft"¹²⁷).
- Kein Subjekt darf das Sicherheits-Niveau eines Objekts verändern ("Störungsfreiheit", "tranquility principle").

Die Bedeutung der einfachen Sicherheitsbedingung liegt auf der Hand; sie ist eine Erweiterung des Objektschutzes durch die Vertrauensstufe. Mit der *-Bedingung wird festgelegt, daß keine Information von einem Objekt höherer Geheimhaltungsstufe auf ein solches mit geringerer übertragen ("deklassifiziert") werden darf. In diesem Kontext sind das Erzeugen und Löschen von Datenbeständen, Signalen und dergleichen als Spezialfälle der Änderung mit eingeschlossen, um zu verhindern, daß Informationen durch das Bitmuster

¹²⁵ Es ist festzustellen, daß auch diese sehr exakte Regelung eine "Lücke" aufweist: es ist nicht vorgesehen, Subjekten nach Kategorie unterschiedliche Vertrauensstufen zuzuordnen. Wenn also beispielsweise der Verwaltungsdirektor eines Krankenhauses auf Grund seiner Aufgabenstellung befugt ist, alle Verwaltungsdaten zu erfahren, und außerdem - wegen der Abwicklung der Kassenanmeldung - auf die Einweisungsdiagnose zugreifen muß, sind ihm - sofern diese Angabe nicht in den Kategorien "Medizin" und "Verwaltung" doppelt geführt werden - damit aufgrund seiner hohen Vertrauenswürdigkeit sämtliche anderen medizinischen Daten zugänglich, obwohl ihm dies von seiner Aufgabe her nicht zukommt.

¹²⁶ Die anderen Forderungen - wie z.B., daß Datenlöschung physikalisch und irreversibel durchzuführen ist - sind allgemeinerer Natur, aber für die hier darzustellende Systematik unerheblich.

¹²⁷ Diese historisch entstandene Bezeichnung wird manchmal durch den Begriff "confinement" ersetzt, der jedoch gelegentlich mit allgemeinerer Bedeutung benutzt wird; s. Lampson [41].

deklassifiziert werden, das etwa das Vorhandensein/Nichtvorhandensein der Elemente einer Objekt-Familie darstellt.

Bei der zunächst einleuchtenden Forderung nach "Störungsfreiheit" ist anzumerken, daß Denning [8] diese gerade nicht fordert, sondern vielmehr "dynamische" Geheimhaltungsstufen definiert. Es muß jedoch auch vermerkt werden, daß der sehr interessante Nachfolgeartikel¹²⁸ von Denning und Denning [9] nur für statische Fälle eine Lösung bietet.

Für ein reales Betriebssystem ist es anscheinend nicht in tragbaren Effizienzgrenzen möglich, die gegenseitigen Abhängigkeiten der Daten im Ablauf eines Anwenderprogramms (d.h. zur Objektzeit) zu verfolgen. Um das Ziel der *-Bedingung nicht zu gefährden, wird diese deshalb meist in dem Sinn verschärft, daß das Verändern eines Objekts verboten wird, wenn *irgendein* Zugriff auf ein anderes mit dominierendem Sicherheits-Niveau stattgefunden haben *könnte*. Am effektivsten wird dies realisiert, wenn man Prozesse oder Prozeßschritte als Subjekte betrachtet, die vom veranlassenden Anwender ein Sicherheits-Niveau zugeordnet bekommen, das von seinem eigenen dominiert wird; dem Prozeß wird dann lesender Zugriff zu allen Objekten gestattet, deren Sicherheits-Niveau von seinem erworbenen dominiert wird, schreibender (einschließlich Erzeugen und Löschen) jedoch nur, wenn die Geheimhaltungsstufe von Objekt und Subjekt *genau gleich* sind. Daß diese Einschränkung die verschärfte *-Bedingung erfüllt, erkennt man, wenn man sich vorstellt, der Anwender würde, um einen Verrat zu begehen, eine temporäre Datei erzeugen; diese müßte danach die derzeitige Vertrauensstufe des Prozesses als Geheimhaltungsstufe erhalten und würde somit "unsichtbar", sobald der Anwender die Vertrauensstufe des Prozesses verringert, um zu versuchen, die Daten in einer geringeren Geheimhaltungsstufe preiszugeben.

Selbstredend muß die *-Bedingung analog dem Objektschutz auf alle Arten von Objekten, also auch Hauptspeicherbereiche und diverse Datenkanäle, angewendet werden; dies ist bei der Interprozessor-Kommunikation eine besonders schwierige Aufgabe. Nach dieser Regelung hat der Erzeuger eines Informationselements nur im Rahmen seines eigenen Sicherheits-Niveaus einen Ermessensspielraum in bezug auf dessen Mehrfachverwendung; es wird genau der Geheimhaltungsstufe und der Kategorie-Menge zugeordnet, mit der der Prozeß zum Zeitpunkt des Erzeugens ausgestattet ist.

Von allen Effizienz-Überlegungen abgesehen, stellen die genannten Bedingungen ein derartig strenges Sicherheitssystem dar, daß es unverändert in der Praxis nicht funktionsgerecht

¹²⁸ Die Sicherstellung des Informationsschutzes wird in die Kompilierzeit verlagert - ein besonders für Datenbanksysteme durchaus erfolgversprechender Ansatz - und es werden Prüfalgorithmen formuliert.

ist; dem Menschen ist jetzt zu wenig Entscheidungsfreiheit verblieben. Aus diesem Grund lassen Bell, Young und die anderen genannten Autoren zwei Ausnahmen gelten:

- "vertrauenswürdige Programme" ("trusted programs") werden von der Prüfung des Sicherheits-Niveaus entbunden, um zentrale Funktionen, wie etwa die Datensicherung (im landläufigen Sinn) oder die Datenwiederherstellung, zu gewährleisten;¹²⁹
- einem Datenschutzbeauftragten ("security officer") wird die Fähigkeit eingeräumt, Daten zu deklassifizieren.¹³⁰

In der Praxis müßten solche Sonderfunktionen ebenso streng überprüft werden wie die Sicherheitsfunktionen des Betriebssystems selbst. Ferner muß sichergestellt werden, daß kein "böses" Programm durch irgendwelche Kanäle auf die entsprechenden Systemschnittstellen zugreifen kann, um selbst die Sicherheitsprüfung zu umgehen. Grundsätzlich ist aber festzustellen, daß diese inhomogenen Ausnahmen eine Verschiebung der Datenschutz- und Datensicherheits-Verantwortung von der Technik weg und zurück zur Organisation darstellen; eine der Praxis nicht angepaßte, zu restriktive Technik kann somit zu einem Rückschlag in den Bemühungen führen, die Organisationsaufgaben im Datenschutz zu minimieren.¹³¹

3.4.3.2 Funktionale Minimalbefugnisse

Das Grundprinzip der Minimalbefugnisse wurde in Abschnitt 3.1 zunächst auf die Benutzer einer DV-Anlage bezogen. Bereits bei der Erläuterung der Zugriffs-Matrix bzw. ihrer Vereinfachung in Form von Ausweisen wurde herausgestellt, daß die Menge der von einem Prozeß "vorgezeigten" Ausweise seine tatsächlichen Befugnisse - bzw. die des veranlassenden Anwenders - i. allg. nur unvollständig wiedergibt. Der Prozeß läuft in einer "Umgebung" ab, die dem gegenwärtigen Bedarf entspricht; er hat einen eigenen Definitionsbereich ("domain"¹³²). Der Gedanke liegt nahe, jeder Prozedur¹³³

¹²⁹ Es handelt sich hier offensichtlich um den Konflikt, der bereits in Fußnote 41 aufgezeigt wurde.

¹³⁰ Z.B. werden statistische, anonymisierte Daten, die aus personenbezogenen Daten gewonnen wurden, nach der *-Bedingung zunächst die selbe Geheimhaltungsstufe wie die Rohdaten erhalten; s. hierzu jedoch Denning, Denning [9], Dobkin et al. [16], Palme [49], Saltzer, Schroeder [62] sowie Abschnitt 2.1.2.

¹³¹ Vgl. hierzu die Anmerkungen über die Akzeptanz von Datenschutzmaßnahmen durch Datenverarbeiter in Abschnitt 2.1.1.

¹³² Lampson [40].

¹³³ Das Wort Prozedur wird hier in Anlehnung an Wulf et al. [80] für einen geschlossenen Programmteil verwendet, der ausführbare Anweisungen enthält und über ein eigenes Datenumfeld verfügt. Ein Prozeß dagegen stellt die gesamte Verarbeitung dar, die mit einer Systemanmeldung eines Benutzers bewältigt wird ("job"), und besteht i. allg. aus mehreren, oft ineinandergeschachtelten Prozedur-Aufrufen.

einen eigenen Definitionsbereich zuzuweisen, und auf diese Weise die Daten zu schützen, die aktuell nicht benötigt werden. Selbstredend muß diese Orientierung am Informations-Bedarf eingeschränkt werden auf das, was der Prozeß bzw. der veranlassende Benutzer *darf*; der Schutz durch funktionale Minimalbefugnisse ersetzt den Objektschutz nicht, sondern ergänzt ihn. Dabei kann es durchaus vorkommen, daß eine Prozedur die Befugnisse des Anwenders auch erweitert.¹³⁴

Man kann zwei Motivkreise unterscheiden, die den Schutz durch Minimalbefugnisse vorteilhaft erscheinen lassen, und die durch folgende Situationen dargestellt werden können:

- Auf ein bestimmtes Objekt (z.B. eine Datei) sollen Programme¹³⁵ ausschließlich über eine spezielle Schnittstellen-Prozedur zugreifen können, die die zulässigen Funktionen definiert. Diese Prozedur kann ggf. auch eine eigene Zulässigkeitsprüfung durchführen und je unterschiedliche Zugriffe gestatten. Offensichtlich darf das aufrufende Programm nicht direkt auf den Definitionsbereich dieser Prozedur zugreifen; denn sonst wären ihm beliebige Manipulationen möglich.
- Ein Programm verwendet eine Prozedur, die ein Dritter zur Verfügung gestellt hat. Der "Besitzer" des Programms mißtraut dieser Prozedur insofern, als er nicht sicher ist, ob sie nicht
 - Daten aus seinem Bereich in einen anderen kopiert, um sie später für eigene Ziele auszuwerten oder zu verraten;¹³⁶
 - einen versteckten Anschluß¹³⁷ enthält, mit dessen Hilfe eine "subversive" Prozedur funktional eingeschleust werden kann,
 - unzuverlässig arbeitet, und somit die Gefahr besteht, daß sie außer Kontrolle gerät und die Daten des aufrufenden Programms (Benutzers) verfälscht oder zerstört.

Diese beiden Fälle entsprechen einer je unterschiedlich gerichteten Vorsicht innerer und äußerer (gerufener und rufender) Prozeduren; selbstredend gibt es auch den Fall des gegenseitigen Mißtrauens. Auf diese Sicherheitsbedürfnisse macht Lampson [40] bereits 1969 aufmerksam und zeigt auch die ersten Ansätze zu einer Lösung auf. Das Thema wird u.a. von Saltzer und Schroeder [62] aufgegriffen und besonders eingehend von Linden [44] behandelt.¹³⁸ Da die erste der genannten Situationen auch den Fall abdecken kann, daß

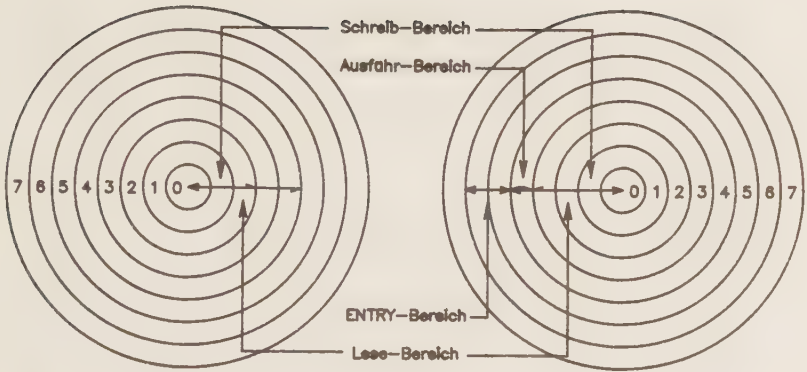
¹³⁴ Diese Möglichkeit sieht auch Young [83] in seiner Sicherheits-Philosophie (s. Abschnitt 3.4.3.1) vor.

¹³⁵ Als Programme sollen solche Prozeduren (s. Fußnote 133) bezeichnet werden, die selbst von keiner anderen Prozedur aufgerufen werden; sie werden unmittelbar von einem Prozeß zur Ausführung gebracht.

¹³⁶ Eine Prozedur mit dieser Eigenschaft wird häufig als "trojanisches Pferd" bezeichnet; s. z.B. Linden [44].

¹³⁷ Solche Mechanismen werden Falltüren ("trap doors") genannt.

¹³⁸ S. auch Lampson [41].



a) Schutzstufen für Daten

b) Schutzstufen für Prozedur

Abb. 8: Ringschutz

Daten vorverarbeitet werden, um ihr Schutzbedürfnis zu senken (z.B. Anonymisierung von personenbezogenen Daten), bevor sie an einen nicht näher zu spezifizierenden Anwender übergeben werden, vermutet Rüdel [60] sogar, daß man sich durch strenge Anwendung der funktionalen Minimal-Befugnisse die oft schwerfälligen Mechanismen des Informationsschutzes ersparen, vor allem aber deren inhomogene Ausnahmeregelungen ("Deklassifizierung" usw.) durch definiertere Verfahren ersetzen kann.

a) Geschützte Subsysteme, Ringschutz

Saltzer und Schroeder [62] nennen Prozeduren, die die Eigenschaften haben, welche in der ersten Situation gefordert wurden, "Geschützte Subsysteme". Sie sind, wie Lampson [40] erkennt, durch eine hierarchische Strukturierung der Subjekte und Objekte relativ leicht zu implementieren, und er prägt den Begriff "Ring" für die einzelnen, hierdurch definierten Schutzebenen.

Das Prinzip des Ringschutzes ist einfach (Abb. 8); der Speicherbereich wird in mehrere, logisch ineinandergeschachtelte Schutzstufen eingeteilt, die monoton durch-numeriert werden - typischerweise von 0 für die sensitivsten, nur dem Betriebssystem unmittelbar zugänglichen Objekte¹³⁹ bis v für ungeschützte. Jeder Benutzer bekommt eine nicht unterschreitbare Schutzstufe aus diesem Intervall zugewiesen, und jedem Prozeß, den er initialisiert, muß er eine gleiche oder geringere zuordnen - ggf. wird implizit die (numerisch) höchste, nur ungeschützte Objekte erfassende Funktionsweise zugelassen; auch mehrfachbenutzbare Routinen ("Reentrante Prozeduren") bekommen Schutzstufen zugewiesen. Objekte tragen ihrerseits

¹³⁹ Z.B. die Liste der Benutzer-Passwörter.

eine Liste mit zunächst zwei Werten R_1 und R_2 , die aus-sagen, ab welcher Schutzstufe eine Prozedur lesend oder verändernd auf die Daten zugreifen darf (Abb. 8a). Da-durch ergeben sich zwei Bereiche: $O-R_1$ für lesenden und $O-R_2$ für verändernden Zugriff, in denen die Prozesse ablaufen müssen, die die Daten benutzen wollen; diese werden als Lese- bzw. Schreib-Bereich oder -Klammer ("bracket") bezeichnet.

Da Prozeduren ebenfalls - ausführbare - Daten darstellen, werden auch ihnen Zugriffsbereiche zugeordnet. Es muß aber ferner definiert werden, in welchen Bereichen sie selbst ablaufen dürfen, d.h. welche Zugriffsrechte an-deren Daten gegenüber sie besitzen. Da sie, um ausführ-bar zu sein, sich selbst - die Maschinenanweisungen - lesen müssen und einen eigenen, veränderbaren Arbeits-bereich benötigen, ist es sinnvoll, den Differenzbereich als Ausführbereich festzulegen, der von R_1 und R_2 (ein-schließlich) begrenzt wird. Da jedoch die Einsprungpunk-te einer Prozedur a priori in der eigenen Ablaufumgebung liegen, ist eine Prozedur nach dieser Festlegung für eine andere nicht ansprechbar, die nicht in diesem Bereich abläuft, d.h. in einem Ring mit Wert $>R_1$. Man definiert deshalb eine weitere Zugriffsart "Aufrufen" ("enter") und legt in den Prozeduren besondere Ein-sprungpunkte ("entries"¹⁴⁰) fest, auf die hiermit zuge-griffen werden darf. Diese neue Zugriffsart bekommt einen eigenen Ring R_3 (Abb. 8b), der je geschützter Pro-zedur extern zum Ring des Lesebereichs (R_1) liegt. Pro-zeduren, die in einem Ring r ablaufen mit $R_3 \geq r > R_1$, dür-fen diese speziellen Einsprungpunkte verwenden, wodurch ihre eigene Schutzstufe temporär auf die der aufgerufe-nen Prozedur angehoben wird. Auf diese Weise

- wird mit dem Aufruf eines solchen "entry" der zu-greifbare Definitionsbereich kontrolliert (d.h. nur solange die aufgerufene Prozedur aktiv ist) erwei-tert;
- können aufrufende Programme unterschiedlicher Schutz-stufen unterschiedlich privilegierte Prozeduren ver-wenden;
- kann verhindert werden, daß ein Programm geringerer Schutzstufe die geschützten Routinen an einem belie-bigen - voraussichtlich schädlichen - Punkt "betritt".

Selbstredend ist der Rücksprung aus einer solchen Proze-dur mit einer Verringerung des Definitionsbereichs auf den ursprünglichen Umfang verbunden.

Der Ringschutz kann sehr effizient mit Hardware reali-siert werden; Schroeder und Saltzer [65] beschreiben

¹⁴⁰ Gelegentlich werden diese speziellen Einsprungstellen, die eine Veränderung des Definitionsbereichs bewirken, auch "gateways" ge-nannt, um sie von den "entries" einfacher Prozeduren, die ohne Erweiterung des Definitionsbereichs ablaufen, zu unterscheiden.

eine Speicherstruktur, die dazu geeignet ist. Der Ringschutz kann jedoch auch - allerdings wesentlich ineffizienter - mit Software implementiert werden; die ersten Versuche dieser Art wurden in Ermangelung geeigneter Hardware programmtechnisch durchgeführt!¹⁴¹

b) Bereichswechsel

Der Ringschutz bewirkt als streng hierarchisches Prinzip lediglich den Schutz von Objekten vor dem unmittelbaren Zugriff durch minderberechtigte Subjekte. Die zweite, zu Anfang dieses Abschnitts geschilderte Situation belegt jedoch, daß auch ein Bedürfnis besteht, *jeder* Prozedur - unabhängig von ihrer Privilegierungsstufe - einen eigenen Definitionsbereich zuzuteilen, der nur die aktuell benötigten Objekte und Berechtigungen enthält. Diese Verschärfung entspricht der von Rüdel [60] geforderten strengen Anwendung des Prinzips der funktionalen Minimalbefugnisse. Linden [44] spricht in diesem Zusammenhang von "kleinen Bereichen" ("small protection domains") und nennt den erforderlichen Mechanismus "Bereichswechsel" ("domain switching"). Wulf und Shaw [81] nennen solche, auf die Prozedur beschränkte Definitionsbereiche "local name spaces" (LNS).¹⁴² Prozeduren, die zu einem Bereichswechsel fähig sind, verfügen in ihrem LNS über zwei unterschiedliche Datenarten:

- Objekte, die ihr selbst "eigen" sind - bzw. allgemeiner einer "Inkarnation" dieser, um Reentranz und Rekursivität zu gewährleisten,¹⁴³ und
- Objekte, die als "Parameter" vom aufrufenden Programm übergeben wurden.

Wulf und Shaw zeigen, daß die gewünschte Funktion sich in einem "capability"-orientierten System verwirklichen läßt, indem

- beim Aufruf einer Prozedur alle bisher den Definitionsbereich kennzeichnenden "capabilities" in einen "Keller" ("stack") geschoben werden,¹⁴⁴
- in diesem Keller je Aufruf eine unüberwindliche "Trennwand" eingezogen wird, die der aktuellen Prozedur jeden Zugriff auf die "capability"-Menge der aufrufenden Prozedur zuverlässig verwehrt!¹⁴⁵

¹⁴¹ Die Hardwaredarstellung des Ringschutzes bezieht sich allerdings ausschließlich auf die geschilderte Situation; beim Sprung in eine Prozedur *niedrigerer* Stufe dagegen müssen vorhandene Befugnisse entzogen und beim Rücksprung wieder zugewiesen werden. Diese Aufgabe konnte nur durch software-technische Maßnahmen gelöst werden.

¹⁴² S. auch Fabry [18].

¹⁴³ Linden [44], Rüdel [60].

¹⁴⁴ Es ist auch bei konventionellen Aufruftechniken notwendig, gewisse Teile des aktuellen Datenumfelds - z.B. die aktuellen Registerstände - zu "kellern".

¹⁴⁵ Genau durch das Vorhandensein solcher Trennwände unterscheidet sich diese Technik von der konventionellen Kellerung.

Obwohl es in diesem Rahmen nicht möglich ist, auf die vielen, hierbei entstehenden Probleme näher einzugehen;¹⁴⁶ sei darauf hingewiesen, daß die Nomenklatur "local name space" anzudeuten scheint, daß Wulf und Shaw in erster Linie an sehr abstrakte Gebilde denken, so daß der "capability"-Begriff hier weiter gefaßt werden muß; vor allem ist bei der sogenannten virtuellen Speichertechnik auch die "Adreß-Umsetztabelle"¹⁴⁷ zu kellern und durch eine neue zu ersetzen, die den Zugriff zum Definitions-bereich der gerufenen Prozedur erst ermöglicht.¹⁴⁸

Der Vollständigkeit halber sei erwähnt, daß Linden, indem er der "capability" ein drittes Unterfeld, "Typ" genannt, beordnet;¹⁴⁹ mit Hilfe des Bereichswechsels eine sehr allgemeine Methode beschreibt, abstrakte Typen durch geschützte Subsysteme zu definieren; doch ist dies eher für die Entwicklung zuverlässiger Software von Belang, als für den Datenschutz im engeren Sinn.

¹⁴⁶ Dazu gehört beispielsweise die Tatsache, daß die Zugriffsberechtigungen eines Prozesses beim parametrischen Übergang von einem Definitionsbereich zu einem anderen ggf. modifiziert werden müssen.

¹⁴⁷ Dies ist eine systeminterne Tabelle, die den "Adreßraum" eines Prozesses definiert, indem sie die Umsetzung virtueller in physikalische Adressen steuert.

¹⁴⁸ Bereits Lampson [40] erkennt, daß der Adreßraum beim Wechsel des Definitionsbereichs miterfaßt werden muß. Popek et al. [54] zeigen, daß die virtuelle Adressierung, der das Paging zugrundeliegt, von anderer Qualität ist als der Zugriff mit "capabilities" im Sinn der bisherigen Definition (Abschnitt 3.4.1.1). Dies erkennt man daran, daß der die Adreß-Umsetztabelle indizierende Teil der virtuellen Adresse vom Anwenderprogramm verändert werden kann. Auch ein Eintrag in die Adreß-Umsetztabelle ist keine "capability"; denn er ist für den Benutzer nicht direkt zugänglich, geschweige denn kopierbar.

¹⁴⁹ Interessanterweise hat Lampson [40] ebenfalls eine Typenfestlegung in der "capability" vorgesehen, dafür aber keine Kennzeichnung der Berechtigungen!

4. VERARBEITUNGSSCHUTZ

4.1 Bedeutung, Definition

In Abschnitt 2.3.2 wurden die Gefahren, die den Datenschutz bedrohen, in fünf Klassen eingeteilt, und es wurde dort und im weiteren Verlauf gezeigt, welcher Art die Maßnahmen sind, die vier von ihnen entgegengestellt werden können:

- der "Zerstörung/Verhinderung" kann nur mit baulichen und organisatorischen Mitteln begegnet werden;
- auch gegen den "Datendiebstahl" wirken - mit Ausnahme der Chiffrierungstechniken, die nicht notwendigerweise datentechnische Methoden im engeren Sinn anwenden¹⁵⁰ - primär organisatorische Vorsorgen;
- die gegen "unberechtigte Systembenutzung" eingesetzten, vornehmlich technischen Mittel wurden in Abschnitt 3.3 unter dem Begriff "Benutzungsschutz" dargestellt;
- das Kernproblem, das dem "unberechtigten/unbeabsichtigten Datenzugriff" zugrundeliegt, wurde schließlich in Abschnitt 3.4 als die Notwendigkeit der Realisierung der kontrollierten Mehrfachverwendung von Daten identifiziert, und es wurden geeignete technische Maßnahmen vorgestellt.

Eine systematische Behandlung der fünften Gefährdung, der "unberechtigten Verarbeitung" liegt dagegen nicht vor. Es handelt sich dabei um die Bedrohung, die davon ausgeht, daß eine vorhandene Zugriffsberechtigung mißbraucht werden kann, um unstatthafte Datenmanipulationen vorzunehmen. Zwar werden Teilaspekte dieser Problematik, auf die noch näher einzugehen sein wird, im Bereich des Informationsschutzes und der funktionalen Anwendung des Prinzips der Minimal-Befugnisse abgedeckt; eine geschlossene und umfassende, theoretische Darstellung fehlt aber anscheinend völlig.

Um diesen Tatbestand richtig würdigen zu können, muß man die Feststellung aus Abschnitt 2.3.3 wiederholen, daß - in der Terminologie der Anlage zu §6 Abs. 1 Satz 1 BDSG - weder die als zentral anzusehende Speicherkontrolle noch die Auftragskontrolle gewährleistet werden können, wenn die unberechtigte Verarbeitung nicht zuverlässig verhindert wird. Sofern ein Betriebssystem keine von den Anwenderprogrammen unabhängige Methode bereitstellt, Zugriffe auf Datenbestände und -kanäle zu protokollieren, ergeben sich auch Umgehungsmöglichkeiten zur Eingabekontrolle und zur Übermittlungskontrolle. Doch auch im nicht-personenbezogenen Bereich der Datenverarbeitung ist die Verhinderung der unberechtigten Verarbeitung von überragender Bedeutung; man

¹⁵⁰ Bei der Chiffrierung wird die Datentechnik höchstens algorithmisch eingesetzt; sie übernimmt keinesfalls eine steuernde Funktion.

muß davon ausgehen, daß gerade diese Form des Vertrauensbruchs einen wesentlichen Anteil an der vielzitierten "Computer-Kriminalität" hat.

In Ermangelung technischer Hilfsmittel werden derzeit folglich vorwiegend organisatorische Wege beschritten, um die unberechtigte Verarbeitung zu verhindern; dazu gehört beispielsweise die strikte räumliche und personelle Trennung zwischen den Stellen, die Anwenderprogramme erstellen, und der ausführenden ("Produktionssteuerung" o.ä.). Solche Maßnahmen können jedoch nur in großen DV-Umgebungen und nur bedingt durchgesetzt werden; fast immer ist in der Einführungsphase eines neuen Softwareprodukts eine diesem Ziel abträgliche, enge Zusammenarbeit erforderlich, und ein geschickter Programmierer wird, wenn er nicht technisch daran gehindert wird, stets eine Umgehung finden. Im Übertragenen Sinn muß es als ein Bruch des Grundprinzips der "offengelegten Methodik" angesehen werden, wenn Datenschutzbestimmungen oftmals den mit der produktiven Abwicklung beschäftigten Personen das Programmieren oder sogar Programmierkenntnisse verbieten.

Bei den vier zuerst angeführten Gefährdungen kann man die eindeutige Tendenz feststellen, mit zunehmender Nähe zur Verarbeitung selbst immer mehr von organisatorischen zu technischen Schutzmaßnahmen überzugehen. Es erscheint widersprüchlich, - und das in diesem Abschnitt bisher Gesagte unterstützt diese Auffassung - daß gerade beim Einsatz der verarbeitenden Mittel ein Rückgriff auf die Organisation stattfindet. Es ist deshalb ein lohnendes Ziel, eine umfassende Theorie und Praxis zur technischen Verhinderung der unberechtigten Verarbeitung zu entwickeln. Diese technischen Mittel sollen mit dem Begriff

"Verarbeitungsschutz"

bezeichnet werden.

4.2 Stand der Technik

4.2.1 Teilaspekte in vorhandenen Theorien

Im vorhergehenden Abschnitt wurde bereits erwähnt, daß der Informationsschutz und die Anwendung der funktionalen Minimalbefugnisse Teilaspekte des Verarbeitungsschutzes abdecken. In der Tat ist der Informationsschutz durch die *-Bedingung geeignet, die - stets auf Verrat zielende - unberechtigte *lesende* Verarbeitung zu verhindern; eine Bekanntgabe oder Übermittlung vertraulicher Daten ist nur an Anwender gleicher oder höherer Vertrauensstufe möglich. Dagegen bleibt die unberechtigte *verändernde* Verarbeitung unberücksichtigt; nichts hindert beispielsweise einen Saboteur daran, ihm zugängliche Daten zu zerstören oder zu verfälschen. Ebenso wird ein ungetreuer Kontenverwalter nicht daran gehindert, betrügerische Transaktionen durchzuführen.

Es muß folglich festgestellt werden, daß der Informationsschutz allein die Forderungen des Verarbeitungsschutzes nicht erfüllt.

Komplexer liegen die Verhältnisse bei der Anwendung des Prinzips der Minimalbefugnisse im funktionalen Bereich. Es ist offensichtlich, daß etwa die "geschützten Subsysteme" in der Lage sind, die Zugriffe auf sensitive Datenbestände zu kanalisieren, wenn man einen anderweitigen Zugriff durch jegliche Anwender¹⁵¹ zuverlässig verhindern kann. Dies ist mit dem Ringschutz möglich, wenn die Daten in einem Ring gespeichert werden, dessen Wert niedriger ist als der aller Anwender. Durch diese Zuordnung kann man u.a. erreichen, daß

- alle Zugriffe lückenlos und mit Angabe des veranlassenden Prozesses oder Anwenders protokolliert werden;
- von einem definierten Ringwert der anfordernden Prozesse an nur solche Daten verfügbar gemacht werden, die durch geeignete Verfahren (Anonymisierung, statistische Vorverarbeitung usw.) desensibilisiert wurden, und damit deklassifiziert werden dürfen;
- auch dem zugriffsberechtigten Anwender nicht beliebige Operationen ermöglicht werden; er hat vielmehr ein "Menü" möglicher, dem legalen Datengebrauch angepaßter Eingriffsmöglichkeiten; dies gilt sowohl für Benutzer, denen verändernder Zugriff gestattet ist, als auch für die, die nur lesend, aber direkt (d.h. in nicht deklassifizierter Form) zugreifen dürfen.

Diese mächtigen Einschränkungen ergeben jedoch noch keinen Verarbeitungsschutz - sie sind höchstens als Unterstützung einsetzbar. Es sei daran erinnert, daß der Verarbeitungsschutz den Mißbrauch der Daten durch *berechtigte* Anwender verhindern soll. Die dritte der oben angeführten Kontrollmöglichkeiten verhindert aber nicht, daß

- der direkt lesebefugte Benutzer die Daten mit einem Programm (beispielsweise über einen Datenfernverarbeitungs kanal) an Dritte verrät;
- ein Änderungsbefugter Anwender über die ihm zugängliche Schnittstelle des geschützten Subsystems Daten verfälscht (ggf. in der Hoffnung, einer Bestrafung entfliehen zu können, bevor die Manipulation entdeckt wird, und die Protokollierung ihn als Schuldigen ausweist); das "klassische" Beispiel des Programms, das die bei Zinsberechnungen anfallenden Rundungsbeträge auf ein dem Programmierer verfügbares Konto überträgt, wird hierdurch nicht generell verhindert.

Auch die Technik der funktionalen Minimalbefugnisse kann

¹⁵¹ Bei den derzeit verfügbaren Betriebssystemen muß hier der Systemverwalter bzw. seine Benutzererkennung ausgenommen werden; s. hierzu Abschnitt 4.5.

folglich nicht als eine Realisierung des Verarbeitungsschutzes angesehen werden.

4.2.2 Die Schlüsselrolle des Programms

4.2.2.1 Das Programm als Gefahrenquelle

Die Gesichtspunkte, die im vorangehenden Abschnitt zu der Erkenntnis führten, daß die Anwendung der funktionalen Minimalbefugnisse nur Teilaspekt des Verarbeitungsschutzes sein kann, geben einen wichtigen Hinweis auf die Ursache, die dieser Unzulänglichkeit zugrunde liegt: es genügt offensichtlich nicht, *Subsysteme*, also Prozeduren, die ihrerseits durch andere aufgerufen werden, zu schützen. Solche inneren Prozeduren der Aufrufhierarchie können in aller Regel von den prozeß-näheren mißbraucht werden, durch die sie aufgerufen werden. Setzt man voraus, daß ein Subsystem korrekt arbeitet, kein "trojanisches Pferd"¹⁵² darstellt und keine "Falltüren"¹⁵³ enthält, so geht die Gefahr des Mißbrauchs stets von den Prozeduren aus, die es aufrufen. Dieser Schluß kann fortgeführt werden bis zu der hierarchisch externen, nur vom Prozeß aufgerufenen Prozedur, dem Programm.¹⁵⁴ Innerhalb der Grenzen, die durch die Zugriffsberechtigungen der Anwender gesetzt werden, kann man mit Programmen jede denkbare Datenmanipulation durchführen. Letztendlich ist es die Summe der Funktionen, die ein Programm darstellt, die die Wirkung auf die Daten ausmacht.

Gallwas et al. [19] sagen: "Daten ... werden zu Informationen durch einen Verarbeitungsprozeß, wozu ein Programm erforderlich ist ... Ohne Programme sind Daten normalerweise nutzlos ...". Daraus kann man schließen, daß eine unerwünschte Ausnutzung von Daten verhindert werden kann, wenn es gelingt, die Anwendung - objektbezogen - unerwünschter Programme zu verhindern. In diesem Kontext muß der Begriff Programm in seiner weitesten Bedeutung verstanden werden. Es ist deshalb von Belang, daß Betriebssysteme, die auf der Ebene der eigenen Sprachoberfläche (JCL, Kommandosprache usw.) *operative* Funktionen bereitstellen,¹⁵⁵ diese mit Hilfe von "versteckten" Dienstprogrammen durchführen.¹⁵⁶

In der Vergangenheit ist das Grundprinzip der "standardmäßigen Zugriffsverweigerung" in bezug auf Programme stets verletzt worden; sofern ein Anwender Zugriffsrechte zu

¹⁵² S. Fußnote 136.

¹⁵³ S. Fußnote 137.

¹⁵⁴ S. Fußnote 135.

¹⁵⁵ Als Beispiel betrachte man das aus Datenschutz-Sicht eminent gefährliche Kopieren von Dateien.

¹⁵⁶ Es ist deshalb konsequent und richtig, wenn die Beschreibung des Betriebssystems NOS von CDC solche Kommandos explizit "Programme" nennt [6].

einem Objekt hat, wird jedem von ihm aufgerufenen Programm dasselbe zuerkannt. Zur Verwirklichung des Verarbeitungsschutzes ist es aber offensichtlich erforderlich, spezifizieren zu können, welche Programme ausschließlich auf ein gegebenes Objekt angewendet werden dürfen.

Um keine unerfüllbaren Erwartungen an den Verarbeitungsschutz aufkommen zu lassen, ist an dieser Stelle eine grundsätzliche Einschränkung zu machen. Auch wenn es gelingt, den Zugriff zu einem Datenbestand auf definierte Programme zu begrenzen, kann die Gefahr des Mißbrauchs mit diesen - etwa durch die Eingabe verfälschter Daten - nicht abgewendet werden. Es ist prinzipiell *technisch* nicht möglich, eingegebene Daten über einige formale¹⁵⁷ und logische¹⁵⁸ Prüfungen hinaus auf ihre Korrektheit zu testen; denn dazu müßte das Programm die Information bereits kennen, wodurch eine Eingabe überflüssig würde. Da die Definition des Verarbeitungsschutzes (s. Abschnitt 4.1) diesen explizit auf technische Verfahren beschränkt, ist diese Gefahr nicht unmittelbarer Gegenstand der vorliegenden Darstellung. Dies schließt keinesfalls aus, daß der Verarbeitungsschutz mittelbar zur Minderung einer solchen Gefährdung beitragen kann, indem etwa bei extrem sensitiven Daten die Einhaltung des "Vier-Augen-Prinzips" erzwungen wird.

4.2.2.2 Unvollständige Lösungsversuche

Die Erkenntnis, daß Programme eine Gefahr für den Datenschutz darstellen, ist nicht neu. So fordern Graham und Denning [22] eine Anzeige im Dateikatalog, die angibt, ob der betreffende Datenbestand kopiert werden darf. Auch Palme [49] führt Dienstprogramme, Editoren usw. als Gefahrenquellen an. Im medizinischen Bereich wird von Griesser et al. [28] eine Programm-Identifikation mit diesem Ziel gefordert.¹⁵⁹ Es gibt deshalb einige Ansätze, die Forderungen des vorangehenden Abschnitts zu erfüllen. Im folgenden sollen drei dieser Versuche geschildert werden, um darzulegen, in welchem Maß und aus welchem Grund sie nicht als vollwertige Verarbeitungsschutz-Methoden angesehen werden können.

Im Rechenzentrum des Deutschen Instituts für medizinische Dokumentation und Information (DIMDI) wird über benutzerbezogene Berechtigungslisten festgelegt, welche Programme dem betreffenden Anwender *nicht* verfügbar sein dürfen.¹⁶⁰ Da diese Regelung, wie in Abschnitt 3.2 bereits dargelegt, das Grundprinzip der standardmäßigen Zugriffsverweigerung verletzt, ist ferner vorgesehen, dem Benutzer alternativ

¹⁵⁷ Z.B. Ausschuß des 30. Februar als Eingabewert.

¹⁵⁸ Eine logische Prüfung liegt vor, wenn Eingabedaten untereinander oder mit bereits gespeicherten Daten in Beziehung gesetzt werden; z.B. darf ein Patient nicht auf die Station verlegt werden, auf der er bereits liegt.

¹⁵⁹ Table 3.10 in Abschnitt 3.4.4.3; ein Verfahren wird nicht angegeben.

¹⁶⁰ Kriener, Michels [39].

eine "Positiv-Liste" der ausschließlich verwendbaren Programme zuzuordnen.

Diese von DIMDI eingesetzte Methode muß - nach einer mündlichen Mitteilung eines leitenden Mitarbeiters dort - als eine "Notmaßnahme" angesehen werden, da eine im Betriebssystem nicht vorgesehene Funktion mit einfachsten Mitteln wenigstens teilweise implementiert werden sollte. Es ist deshalb auch nicht verwunderlich, daß sie einige schwerwiegende Mängel aufweist:

- Es werden nicht - wie gefordert - Programme mit Objekten in Verbindung gesetzt, sondern Programme und Anwender.¹⁶¹ Dadurch ist eine differenzierte Steuerung gegenüber den Datenbeständen und ihren individuellen Schutzbedürfnissen nicht möglich. Folglich muß dem Benutzer die Berechtigung zuerkannt werden, die seinen *maximalen* Bedürfnissen entspricht - ein Widerspruch zum Grundprinzip der minimalen Befugnisse.
- Als Folge dieser Tatsache ergibt sich, daß die Mitarbeiter mit den weitesten Zugriffsrechten - von denen die größte Gefahr der unberechtigten Verarbeitung ausgeht - praktisch globale Berechtigung gegenüber der Programmanwendung haben müssen; der Mechanismus wirkt nur bei den weniger privilegierten Anwendern, die von Haus aus nur geringe Zugriffsrechte besitzen.

Trotz des offensichtlichen Ziels, die Verwendung von Programmen zum Zwecke des Datenschutzes einzuschränken, kann das vom DIMDI eingesetzte Verfahren nicht als Realisierung des Verarbeitungsschutzes angesehen werden.

Die beiden anderen Verfahren, die eine Einschränkung der auf einen Datenbestand anwendbaren Programme zum Ziel haben, stellen sich als Extremfall des Schutzes durch geschützte Subsysteme dar, indem diese Programm-Charakter annehmen. Diese speziellen Programme besitzen eigene Zugriffs-Berechtigungen, die dem - i. allg. weniger privilegierten - Anwender temporär übertragen werden können. Diesen Vorschlag findet man bei Young [83], der im Rahmen der bereits in Abschnitt 3.4.3.1 vorgestellten "Sicherheits-Philosophie" eher beiläufig erwähnt, man könne Programmen eine Zugriffs-Kontrollliste beigeben, die die Datenbestände aufzählt, über die sie delegierbare Zugriffsrechte besitzen.¹⁶² Dies setzt natürlich voraus, daß die betreffenden Datenbestände ausschließlich durch die genannten Programme zugreifbar sein dürfen, wenn ein Verarbeitungsschutz erreicht werden soll;

¹⁶¹ In der Nomenklatur der Zugriffsmatrix müßte von Subjekt-Subjekt-Beziehungen gesprochen werden; dies darf nicht mit der Objekt-Eigenschaft der Subjekte verwechselt werden, bei der die mittelbare Wirkung auf ein weiteres Objekt nicht in Betracht gezogen wird.

¹⁶² Diese Darstellungsweise ist typisch für Young, der - in der Literatur anscheinend einmalig - die Zugriffs-Kontrolllisten den *Subjekten* zuordnet, ohne die einhergehenden Probleme zu analysieren.

eine Forderung, die Young *nicht* stellt. Der Verfasser konnte auch keinen Hinweis auf eine Realisierung dieser Methodik finden. In der Wirkung sehr ähnlich dürfte jedoch ein Mechanismus sein, der im System VAX/VMS von Digital Equipment eingebettet ist [12]. In diesem Betriebssystem kann der Systemverwalter speziellen Programmen bzw. ihren einzelnen, in Dateien gespeicherten Ausprägungen ("known images",¹⁶³ "bekannte Programmdateien") beliebige Privilegien erteilen, die sie - streng auf ihre Objektzeit beschränkt - dem aufrufenden Benutzer übertragen können. Da VAX/VMS den Zugriff zu Dateien durch entsprechende Privilegierungen kontrolliert, können solche Programme dem Anwender aktuell Datenzugriffe ermöglichen, die ihm unter anderen Umständen verwehrt würden.

Einen völlig anderen Weg beschreitet das Series 1100 Security System von Sperry Univac [69]. Diese Betriebssystemerweiterung sieht neben den "normalen" Dateien, auf die mit einem allgemein zugänglichen Datenverwaltungssystem zugegriffen wird, auch eine spezielle Art vor, die nur mit einem getrennten Ein-/Ausgabeverfahren angesprochen werden können. Dieses besondere Zugriffsverfahren kann seinerseits nur aufgerufen werden von Programmen, die der Systemverwalter in eine definierte, systemweit einmalige und gegen sonstige Veränderung geschützte Bibliothek eingebracht hat.

Ohne anderweitige Anwendungsmöglichkeiten auszuschließen, muß festgestellt werden, daß sowohl die Strategie von Digital Equipment, als auch die von Sperry Univac offensichtlich pragmatisch auf das in Abschnitt 2.3.2.5 dargestellte Problem gerichtet sind, daß verschieden berechnete Benutzer mit einem Datenbanksystem arbeiten müssen, dessen Einzelinformationen unterschiedliche Schutzbedürfnisse aufweisen. Die mit einer dieser Methoden privilegierten Programme müssen folglich im allgemeinen eigene Kontrollmechanismen enthalten, um die realen Berechtigungen des aktuellen Benutzers zu prüfen, und ggf. dessen Verarbeitungsmöglichkeiten einzuschränken. In der Tat bietet Sperry Univac als weiteren Zusatz zu dem Security System leistungsfähige Software-Hilfen [70], die über eine Steuerung der geschützten und ungeschützten Felder in Bildschirmmasken die Verwirklichung der *-Bedingung des Informationsschutzes programmintern und datenbankbezogen - d.h. bis zur Feldebene hinunter - ermöglichen.

Zweifellos erfüllen die beiden zuletzt dargestellten Verfahren Aufgaben des Verarbeitungsschutzes; denn sie grenzen die Verfahren ein, die auf spezifizierte Datenbestände angewandt werden können. Es läßt sich aber nicht übersehen, daß sie - im Gegensatz zu den in Abschnitt 3.4 geschilderten Verfahren - ausschließlich pragmatischer Natur sind. Sie

¹⁶³ Solche Programme dürfen trotz der identischen Privilegierungstechnik nicht mit den "trusted programs" des Informationsschutzes verwechselt werden; sie stehen nicht nur der Systemverwaltung, sondern im Prinzip allen Benutzern zur Verfügung.

zielen auf ein Einzelproblem, ohne eine systematische Basis zu haben, und folglich mangelt es ihnen an Allgemeingültigkeit:

- Die Verfahren wirken nur bei speziellen Datenbeständen, die auf eine nicht näher definierte Weise gegen jeden Zugriff außer über die bevorrechtigten Programme geschützt werden müssen; in der Regel werden sie in einer Benutzererkennung oder in einem Ring angelegt werden müssen, die nur dem Datenschutzbeauftragten zugänglich ist.¹⁶⁴
- Bei der Methode von Digital Equipment ist die Berechtigungsinformation dem Programm zugeordnet; dieses muß die entsprechenden Privilegien als statische Bestandteile enthalten: die Möglichkeit, dynamisch - also zur Objektzeit - zu bestimmen, für welche Datei die erweiterten Zugriffsrechte gelten, würde dem aufrufenden Anwender den Zugriff zu sämtlichen gleichorganisierten und gleichstrukturierten Datenbeständen eröffnen. Die statische Zuordnung eines definierten Datenbestands zu einem Programm ist jedoch eine schwerwiegende Einschränkung, die meist nicht hingenommen werden kann; vor allem bedeutet sie, daß das Programm nicht anderweitig verwendet werden kann, auch wenn dies sinnvoll wäre.
- Beim Verfahren von Sperry Univac schließlich wird eine Mehrzahl ("pool") von nicht notwendigerweise logisch zusammenhängenden Datenbeständen (alle Dateien, die nur mit der speziellen Datenzugriffsmethode ansprechbar sind) einem "pool" der berechtigten Programme (die Spezialbibliothek) zugeordnet; es fehlt die spezifische Bindung der einzelnen Datenbestände an "ihre" Programme. Die Folge ist, daß beide Mengen recht klein gehalten werden müssen, um den Schutzeffekt nicht zu gefährden.

Gerade der zuletzt genannte Umstand zeigt ein Dilemma auf, das - in subtilerer Form - auch der Technik von Digital Equipment anhaftet: es ist auch dort umständlich und gefährlich, eine größere Anzahl von Dateien gegen unberechtigte Verarbeitung zu schützen; denn hier wächst die Zahl der privilegierten Programme leicht in unkontrollierbare Größen hinein. Die Erfahrung lehrt jedoch, daß gerade von den vielen in großen DV-Anwendungen benötigten Neben- und Hilfsdateien (Eingabedateien, Zwischendateien für Sortiervorgänge, Warteschlangen zur Pufferung, Druckdateien, Prozedurdefinitionen usw.) Gefahr droht. Wegen ihrer scheinbar sekundären Bedeutung gegenüber den zentralen Haupt-Datenbeständen wird ihr Schutz oft vergleichsweise geringer beachtet - ein Umstand, den der versierte "Angreifer" sehr wohl auszunutzen versteht. Ein Schutzmechanismus, der sich darauf beschränken muß, eine oder wenige Datenbestände zentraler Bedeutung zu schützen, bietet folglich nicht gene-

¹⁶⁴ S. auch Fußnote 151.

rell die erforderliche Sicherheit.

Der eigentliche Grund für die Unhandlichkeit der geschilderten Verfahren bei einer größeren Anzahl zu schützender Dateien ist darin zu erkennen, daß diese einen herausgehobenen Status erhalten müssen. Dies ergibt sich daraus, daß die Befugnisse der Anwender und der Programme *additiv*¹⁶⁵ verknüpft werden; die Anwender dürfen folglich keinerlei eigene Befugnisse den Daten gegenüber besitzen, wenn diese ausschließlich mit den spezifizierten Programmen bearbeitet werden sollen. Daraus folgt, daß ein benutzerbezogener Schutz der Daten nicht mehr durch direkte Anwendung des Objektschutzes erfolgen kann. Vielmehr wird die Zugriffsberechtigung zu den Daten auf die Befugnis abgebildet, die bevorrechtigten Programme auszuführen, sowie ggf. auf deren Fähigkeit, selbst den aktuellen Anwender zu erkennen und davon abhängig unterschiedliche Funktionen bereitzustellen.

4.3 Allgemeine Systematik

4.3.1 Die dreidimensionale Zugriffsmatrix

Die vorstehende Analyse des Stands der Technik hat gezeigt, daß die Verfahren, die bislang angewandt wurden, um Funktionen des Verarbeitungsschutzes zu verwirklichen, weder als allgemeingültig angesehen werden können, noch zum Schutz einer größeren Anzahl unterschiedlicher Datenbestände geeignet sind. Es versteht sich aber von selbst, daß eine generelle Systematik in der Lage sein muß, den Zugriff zu beliebigen Daten auf beliebige, spezifizierte Programme einzuschränken. Die Konsequenz aus dieser Forderung ist, daß die Funktion des Objektschutzes für alle gegen unbe-rechtigte Verarbeitung zu schützenden Daten erhalten bleiben muß: sie müssen in beliebigen Benutzerkennungen angelegt sein können. Die Funktionen des Verarbeitungsschutzes müssen den Objektschutz erweitern. Man kann dies auch so formulieren, daß die Zugriffsberechtigungen von Anwendern und Programmen *multiplikativ*¹⁶⁶ verknüpft werden müssen.

Der Umstand, daß sowohl die Befugnisse der Anwender wie die der Programme zur Feststellung der Zugriffsrechte unabhängig voneinander herangezogen werden, führt zu einer neuen Dimension der Zugriffsmatrix: stellte diese in allen bisher bekannten Darstellungen einen zweidimensionalen Zusammenhang zwischen Subjekten und Objekten dar, so kommt nun das von dem Subjekt angewandte Verfahren als weiteres Kriterium hinzu; der Zugriff zum Datenbestand ist von zwei unabhängigen Faktoren abhängig. Die objektbezogene Spalte, in der die Befugnisse der einzelnen Subjekte bislang festge-

¹⁶⁵ Ein Zugriff ist gestattet, wenn der Anwender oder das Programm die erforderliche Befugnis besitzt.

¹⁶⁶ Ein Zugriff ist nur gestattet, wenn der Anwender und das Programm beide die erforderlichen Befugnisse besitzen.

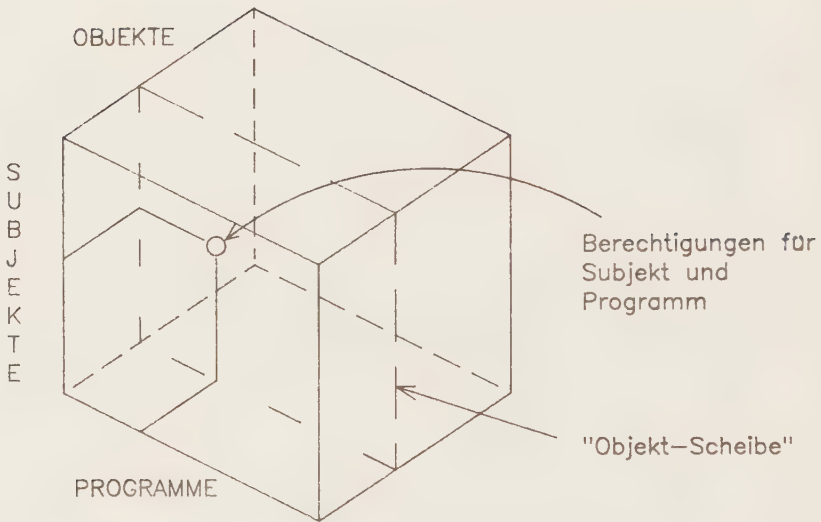


Abb. 9: Zugriffsmatrix für Verarbeitungsschutz

halten sind, erweitert sich zu einer Scheibe (Abb. 9), deren Gitterpunkte die Befugnisse sowohl der Subjekte (Anwender) wie der Verfahren (Programme) enthalten.

In Abschnitt 3.4.2 wurde festgestellt, daß die - zweidimensionale - Zugriffsmatrix in der dargestellten Form nicht als Steuerungsmittel geeignet ist; sie stellt einen "abstrakten Sicherheitszustand" dar und muß strukturell vereinfacht werden, um funktional eingesetzt zu werden. Dies gilt natürlich in erhöhtem Maß für das um eine Dimension erweiterte Gebilde. Ein erster Schritt zu einer solchen Reduktion ergibt sich aus der Feststellung, daß die vollständige dreidimensionale Zugriffsmatrix die Möglichkeit beinhaltet, die Zugriffsberechtigungen eines Verfahrens auf ein definiertes Objekt von dem aktuellen Anwender abhängig zu machen und umgekehrt.¹⁶⁷ Diese Allgemeinheit ist in der Praxis nicht erforderlich; denn die Verfahren sind ja ebenfalls Objekte (die Programme werden in Dateien abgelegt¹⁶⁸), so daß diese Abhängigkeit durch das Recht des betreffenden Anwenders verwirklicht werden kann, das Programm auszuführen. Anders ausgedrückt besagt dies, daß Gitterpunkte der Objektscheibe in einer dreidimensionalen Zugriffsmatrix,

¹⁶⁷ Für diese Abhängigkeit wurde in Fußnote 161 noch die Bezeichnung "Subjekt-Subjekt-Beziehung" verwendet.

¹⁶⁸ Zu diesen speziellen Objekten haben in der Verfahrensdimension im allgemeinen nur die Dienstprogramme Zugriffsbefugnis, die sie binden, laden oder allenfalls kopieren.

Katalog

...		
DAT-PAT	zugelassene Benutzer	zugelassene Programme
Adresse	Maier lesen/verändern	PROG-A lesen
PROG-A	zugelassene Benutzer	zugelassene Programme
Adresse	Maier ausführen	-----
Kennwort	Müller ausführen	
DAT-PERS	zugelassene Benutzer	zugelassene Programme
Adresse	Müller lesen/anfügen	PROG-A lesen PROG-X anfügen
...		

Abb. 10: Zugriffs-Kontrollliste
für Verarbeitungsschutz

die sich auf dasselbe Subjekt oder Verfahren beziehen, identische Befugnisse für das Objekt enthalten!⁶⁹

Diese Eigenschaft der Verfahren, daß sie - ebenso wie die Subjekte - auch als Objekte angesehen werden können, ermöglicht es, ähnliche Vereinfachungen durchzuführen, wie sie sich im zweidimensionalen Fall bewährt haben:

- Die Auflösung der Zugriffsmatrix in die einzelnen Objektscheiben ergibt eine Listenstruktur, wenn man alle leeren Einträge eliminiert. Allerdings sind jetzt je eine Zugriffskontrollliste für Subjekte (Benutzer) und Verfahren (Programme) vorzusehen (Abb. 10).
- Die weitere Auflösung in einzelne, nicht leere Matrixpunkte ergibt auch hier eine ausweisorientierte Struktur. Dazu ist es aber erforderlich, die Adressierungsfunktion auf zwei einander eindeutig zugeordnete "capabilities" aufzuteilen: je Objekt darf eine Adres-

¹⁶⁹ Allenfalls könnte dem "Besitzer" der Daten ein Recht zugestanden werden, die Daten mit weiteren oder beliebigen Programmen zu verarbeiten.

se nur aus den Informationsinhalten beider "capabilities" zusammen feststellbar sein!¹⁷⁰ Selbstverständlich muß Sorge getragen werden, daß weder ein Subjekt noch ein Verfahren über zwei sich ergänzende "capabilities" verfügen kann: eine Anzeige muß diese eindeutig den Subjekten oder Verfahren zuordnen.

Es darf angenommen werden, daß eine Aufspaltung des Adressierungsmechanismus auf zwei zusammenwirkende "capabilities" wesentlich tiefere Eingriffe in die Systemarchitektur bedingen müßte, als die Erweiterung der Zugriffs-Kontrolllisten um eine zweite Aufstellung, die - wie noch zu zeigen sein wird - in einer getrennten Katalog-Ergänzungsdatei geführt werden kann. Selbstredend ist auch ein Mischsystem denkbar, bei dem ein auf "capabilities" aufbauendes System mit verfahrensbezogenen Zugriffskontrolllisten "nachgerüstet" wird. Wegen dieser vergleichsweise einfacheren Ergänzungsmöglichkeit bestehender Systemarchitekturen soll im folgenden nur noch die listenorientierte Erweiterung des Objektschutzes betrachtet werden, obwohl alle Ergebnisse auch auf ein System mit "capability"-Paaren übertragbar wären.

4.3.2 Programm-Identifikation und -Authentifikation

Die Forderung, Datenbeständen Listen zuordnen zu können, die angeben, welche Programme sie verarbeiten dürfen, ist in sich nicht neu. Sie wird aber stets begleitet von dem resignierenden Hinweis, daß man sich gegen eine Verfälschung der Programme praktisch nicht wehren kann, vor allem, wenn man sich die Möglichkeiten der höherprivilegierten Mitarbeiter vor Augen hält!¹⁷¹

Die bestechende Symmetrie zwischen Benutzer und Programm in der im vorhergehenden Abschnitt vorgestellten, neuen Gestalt der Zugriffskontrollliste gibt einen Hinweis auf die Lösung des Problems; sie besteht nämlich in Wirklichkeit nur optisch; Benutzer und Programme werden bisher ganz und gar unterschiedlich behandelt, wenn es darum geht, Sicherheit zu gewinnen. Während sehr viel Mühe darauf verwendet wurde, Methoden zu entwickeln, um das Eindringen eines nicht zugelassenen Benutzers zu verhindern (s. Abschnitt 3.3, Benutzungsschutz), werden Programme bzw. ihre Ausprägungen in Dateien (Lademoduln, Phasen, "images" usw.) zwar als schützenswerte Objekte behandelt, in ihrer aktiven Rolle als verarbeitende Verfahren jedoch fraglos akzeptiert. Um eine echte Symmetrie herzustellen, ist es folglich notwendig, die zugriffsberechtigten Programmausprägungen eindeutig zu identifizieren und eine Möglichkeit zu schaffen, sie auch zu authentifizieren, um sicherzustellen, daß

¹⁷⁰ Diese Funktionsaufteilung läßt sich vergleichen mit dem Vier-Augen-Prinzip oder dem Verfahren, daß ein Tresor sich nur mit zwei getrennt aufzubewahrenden Schlüsseln öffnen läßt.

¹⁷¹ S. auch das in Abschnitt 2.3.2.5 erläuterte "Versions-Problem".

Katalog

. . .		
DAT-PAT	zugelassene Benutzer	zugelassene Programme
Adresse	Maier lesen/verändern	PROG-A lesen
PROG-A	zugelassene Benutzer	zugelassene Programme
Adresse	Maier ausführen	---
Kennwort	Müller ausführen	
DAT-PERS	zugelassene Benutzer	zugelassene Programme
Adresse	Müller lesen/anfügen	PROG-A lesen
		PROG-X anfügen
. . .		

Benutzer-ID-Liste

. . .	
Maier	Passwort
Müller	Passwort
Schmidt	Passwort
. . .	

Programm-ID-Liste

. . .	
PROG-A	Soll-Kennwort
PROG-N	Soll-Kennwort
PROG-X	Soll-Kennwort
. . .	

Abb. 11: Zugriffs-Kontrollliste und ID-Listen für Verarbeitungsschutz

sie nicht durch "subversive" Funktionen ersetzt oder ergänzt wurden. So wie die auf den Objektschutz beschränkte Wirkung der zweidimensionalen Zugriffsmatrix völlig von der Zuverlässigkeit des Benutzungsschutzes abhängig ist, ist die erweiterte Form für den Verarbeitungsschutz auf eine sichere Feststellung der Identität der angewendeten Verfahren angewiesen. Um den Verarbeitungsschutz verwirklichen zu können, muß also die beobachtete Symmetrie über die Zugriffskontrolllisten hinaus auf die Identifikationslisten ausgedehnt werden (Abb. 11), wobei nicht nur eine namensmäßige Kontrolle stattfinden muß, sondern auch eine echte Authentifikation¹⁷²

Der Verarbeitungsschutz wird gewährleistet, wenn

- der Objektschutz derartig ausgeweitet wird, daß die Befugnisse von Subjekten und wirksamen Verfahren unabhängig und multiplikativ zur Feststellung der Zugriffsberechtigung herangezogen werden, und
- wenn die Verfahren ebenso wie die Subjekte, die sie anwenden, identifiziert und authentifiziert werden können.

Daß und wie dies erreicht werden kann, soll im folgenden Abschnitt 4.4 ausführlich dargestellt werden.

4.4 Realisierung

4.4.1 Rahmenbedingungen

4.4.1.1 Betriebssystem

Die Realisierung des Verarbeitungsschutzes, die in diesem Abschnitt vorgestellt werden soll, konnte naturgemäß nur im Rahmen eines vorhandenen Betriebssystems erfolgen und mußte auf dessen Möglichkeiten und Unzulänglichkeiten abgestimmt werden. Die vorliegenden Ergebnisse wurden auf einer DVA der Firma Siemens unter dem Betriebssystem BS2000 [68] erarbeitet. Diese sieht die Möglichkeit vor, Dateien durch Kennwörter zu schützen; es können verschiedene Kennwörter definiert werden, um lesenden oder verändernden Zugriff auf Dateien zu gestatten, bzw. um sie auszuführen (als Programm oder Prozedur) zu ermöglichen. In BS2000 ist diese Funktion nicht als Erweiterung des Grundschutzes der Daten anzusehen, sondern als eine absolute Notwendigkeit; denn ansonsten ist

¹⁷² Es ist eine Frage der Betrachtungsweise, ob man im Fall der in Abschnitt 4.2.2.2 erläuterten Vorgehensweisen von Digital Equipment und Sperry Univac feststellt, daß sich hier eine Authentifikation wegen der Sonderstellung erübrigt, die der Systemverwalter dem privilegierten Programm erteilt, oder ob man diese Privilegierung gerade als eine implizite Authentifikation auffaßt; keinesfalls wird hierdurch die Feststellung betroffen, daß es sich bei beiden Methoden um pragmatische, in ihrer Wirkung und Allgemeingültigkeit begrenzte Mittel handelt.

nur eine globale Mehrfachbenutzung definierbar; d.h. der Besitzer eines Datenbestands kann diesen nur einem anderen zur Verfügung stellen, wenn er ihn der ganzen Nutzergemeinde verfügbar macht. Saltzer und Schroeder [62] zählen Betriebssysteme mit dieser Eigenschaft überhaupt nicht zur Kategorie der kontrollierten Mehrfachbenutzung¹⁷³ und aus dieser Sicht stellt der Schutz durch Kennwörter die einzige Möglichkeit dar, die global-permissive Behandlung aller mehrfachverwendbaren Datenbestände einzuschränken. Wenn die Verwendung von Datei-Kennwörtern in Abschnitt 3.4.1.1 als "zweite Verteidigungslinie" bezeichnet wurde, dann ist hier festzuhalten, daß es im BS2000 für mehrfachverwendbare Datenbestände keine "erste Verteidigungslinie" gibt.

Die Aussage in Abschnitt 3.3, daß das Passwort als unsicheres Mittel zur - alleinigen - Realisierung des Benutzungsschutzes bekannt ist, gilt in noch höherem Maße für Datei-Kennwörter¹⁷⁴:

- der einzelne, mit sensitiven Daten befaßte Anwender muß eine große bis unübersehbare Anzahl solcher Kennwörter behalten, wenn er nicht immer dasselbe verwenden¹⁷⁵ oder sich schriftliche Aufzeichnungen machen will;
- im allgemeinen müssen Kennwörter vielen Personen bekannt sein; denn sonst gäbe es auch wenig Grund, die Datenbestände mehrfachverwendbar zu machen.¹⁷⁶

Beide Tatsachen machen es einem potentiellen Angreifer außerordentlich leicht, wenn er planmäßig vorgeht; der Schutz wirkt praktisch nur gegen den versehentlichen unbefugten Zugriff. Vor allem die erstgenannte Gefahrenquelle gewinnt weiter an Bedeutung, wenn man als Subjekt nicht menschliche Benutzer, sondern Prozeduren in Betracht zieht: abgesehen davon, daß bereits das Erstellen der Prozedur ein schriftliches Festhalten des Kennworts (in einer Textdatei) darstellt, muß nunmehr auch die Prozedur selbst geschützt werden, um den Mißbrauch der ursprünglich zu schützenden Daten zu verhindern!¹⁷⁷ Auf diese Weise kommt eine Kaskadie-

¹⁷³ S. Fußnote 106

¹⁷⁴ S. Fußnote 102.

¹⁷⁵ Dies setzt allerdings voraus, daß er der "Besitzer" der Daten ist, und es ist natürlich sehr gefährlich, da ein bekanntgewordenes Kennwort den Zugriff zu einer Vielzahl von Datenbeständen freigibt.

¹⁷⁶ Als Ausnahme ist der Fall anzuführen, bei dem der Besitzer einer Datei globalen Lesezugriff gestatten möchte, sich selbst jedoch den verändernden Zugriff durch die Vergabe eines Schreib-Kennworts vorbehält.

¹⁷⁷ Es muß als schwerwiegender Fehler eines Betriebssystems angesehen werden, wenn ein Anwender beim Anlegen neuer Dateien die bislang an dieser Speicherstelle gespeicherten Daten einsehen kann; diese Situation wäre - nicht nur im Hinblick auf Datei-Kennwörter und Passwörter - ein unüberwindliches Hindernis für einen effektiven Einsatz irgendwelcher Datenschutzmaßnahmen.

rung von Schutzbedürfnissen zustande, die nur noch mit großem Aufwand bewältigt werden kann. Das Aufspüren solcher und ähnlicher Fälle indirekter¹⁷⁸ Gefährdung gehört zu den mühsamsten Aufgaben eines Datenschutzbeauftragten, die in regelmäßigen Abständen durchzuführen sind.

4.4.1.2 Das Prinzip der unbekannten Datei-Kennwörter

In der im vorangehenden Abschnitt dargelegten Situation und mit den schwerwiegenden Datenschutzanforderungen der Medizin konfrontiert, hat der Verfasser bereits vor Jahren begonnen, nach Wegen zu suchen, auf möglichst einfache Weise dem Betriebssystem BS2000 Benutzergruppen-Strukturen "aufzusetzen", um eine gezieltere Mehrfachverwendbarkeit für schutzwürdige Daten zu erreichen. Zu diesem Zweck war es erforderlich, eine Erweiterungsdatei zu der Liste der zugelassenen Benutzer¹⁷⁹ einzurichten, und einen Monitor mit der Aufgabe zu betrauen, die Zulässigkeit eines Zugriffs auf eine Datei (genauer: des Eröffnens) an Hand der dort gespeicherten Strukturdaten zusätzlich zu prüfen. In Abschnitt 3.2 wurde bereits dargelegt, daß ein System nicht als sicher angesehen werden kann, wenn es einen Weg gibt, unter Umgehung des Monitors auf geschützte Daten zuzugreifen, und diese Tatsache stellte zur damaligen Zeit¹⁸⁰ ein erhebliches Problem dar.

Die Schwierigkeit konnte durch die folgenden, einfachen Überlegungen überwunden werden:

- es ist möglich, einer Datei Schreib- und/oder Lese-Kennwörter durch ein Programm zuweisen zu lassen; dieses kann solche Bitkombinationen willkürlich¹⁸¹ auswählen, ohne sie - etwa durch Protokollierung - bekanntzugeben;
- damit wäre zunächst der Zugriff auf eine solche Datei jedermann verwehrt;
- somit könnte ein Monitor, der auf irgendeine Weise den Schutz gezielt ausschalten kann, selbst nicht umgangen werden.

Dieser Monitor muß offensichtlich mit denselben Privilegien wie das Betriebssystem selbst ausgestattet sein, damit er die Datei-Kennwörter aus dem Katalog erfragen kann. Er kann dann diese einem Anwender nach positiv verlaufener Berechtigungsprüfung vorübergehend - d.h. ausschließlich für den einen Vorgang - verfügbar machen, damit dieser die Datei

¹⁷⁸ S. hierzu auch Abschnitt 4.2.2.2.

¹⁷⁹ In BS2000 wird diese Datei JOIN-File genannt.

¹⁸⁰ Die sogenannten System-Exits des BS2000 sind erst mit der Version 7.1 freigegeben worden; diese ermöglichen es einem Rechenzentrum, eigene Kontroll- und Steuer-Routinen an ausgezeichnete Stellen ins Betriebssystem einzubinden.

¹⁸¹ Beispielsweise durch einen guten (Pseudo-)Zufallszahlen-Generator (s. Knuth [38]).

eröffnen kann. Dieses neue Verfahren wird als das

Prinzip der unbekannten Datei-Kennwörter

bezeichnet.

Daß dieses Verfahren nur im Rahmen von Betriebssystemen angewendet werden kann, die Dateien mit Kennwörtern schützen lassen, versteht sich von selbst; die Wirksamkeit ist aber auch davon abhängig, daß

- Kennwörter nur unter Angabe des bisherigen Werts verändert werden können,
- auch der Besitzer einer Datei die zugehörigen Kennwörter nicht vom Betriebssystem erfragen kann.

Beide Bedingungen sind im BS2000 erfüllt!¹⁸² Darüber hinaus bietet BS2000 die Option, Pass- und Kennwörter intern in quasi-irreversibel verschlüsselter Form zu halten, wodurch die Sicherheit signifikant erhöht wird¹⁸³; denn dann ist es unschädlich, wenn sie in Speicherabzügen sichtbar werden, oder wenn es einem Angreifer gelingt, direkt auf die Katalogdatei zuzugreifen. In der vorliegenden Anwendung bleiben die Kennwörter unter allen Umständen unbekannt.

Die gezielte Einschränkung der Mehrfachverwendbarkeit von Dateien mit Hilfe des Prinzips der unbekannten Datei-Kennwörter ist beibehalten worden, auch nachdem System Exits¹⁸⁴ für den Betreiber von BS2000 verfügbar wurden; denn dieses Verfahren bietet einen grundsätzlichen Vorteil. Es ist nämlich möglich, die System Exit-Routinen zu entladen. Obwohl die Befugnis hierzu ausschließlich beim Systemverwalter liegt, muß man damit rechnen, daß es einem Angreifer gelingen könnte, diese Deaktivierung gezielt zu provozieren. Ist nun einer solchen Exit-Routine allein die Aufgabe übertragen worden, den Zugriffswunsch auf eine mehrfachverwendbare Datei an Hand der Gruppenzugehörigkeit des veranlassenden Anwenders zusätzlich zu überprüfen, versagt die zusätzliche Eingrenzung, sobald diese zusätzliche Systemkomponente außer Betrieb gesetzt wird. Wird dagegen der Monitor zur Realisierung des Prinzips der unbekannten Datei-Kennwörter durch irgend eine Ursache unwirksam, so entfällt jede Möglichkeit (auch für den eigentlich Berechtigten!), die betreffenden Bestände zu eröffnen; denn nun ist keinerlei Möglichkeit mehr geboten, den Kennwortschutz zu lockern. Das Grundprinzip der standardmäßigen Zugriffsverweigerung ist - im Gegensatz zu der Lösung mit System Exits - stets gewahrt.

Mit diesem neuen Verfahren wird dem Anwender die Möglichkeit genommen, eigene Datei-Kennwörter zu definieren, um seine Datenbestände zu schützen - zumindest, wenn es sich um Dateien handelt, die nur innerhalb der Gruppenstruktur

¹⁸² Das Betriebssystem NOS von CDC beispielsweise verletzt die zweite Forderung mit der CATLIST-Anweisung.

¹⁸³ S. auch Fußnote 70.

¹⁸⁴ S. Fußnote 180.

mehrfachverwendbar sein sollen. Der Verzicht auf diese Funktion fällt aber leicht angesichts der dargestellten schwachen und angreifbaren Schutzwirkung eines konventionell verwendeten Kennworts, zumal dieses durch die neue Verwendungsart eine unvergleichbar mächtigere, global gültige Funktion erhält.

4.4.2 Methodik

In Abschnitt 4.3.2 wurde dargelegt, daß der Verarbeitungsschutz verwirklicht werden kann, wenn man Programme

- identifizieren und
- authentifizieren

kann. Die Identifikation stellt keine grundsätzlichen Probleme; es ist lediglich erforderlich

- eine zusätzliche Datei einzurichten, die - analog zur Liste der zugelassenen Anwender - den Dateien, in denen zugriffsberechtigte Programme gespeichert sind, Identifikationsnamen zuordnet;
- eine Erweiterung des Katalogs zu schaffen, die die programmbezogenen Zugriffs-Kontrolllisten enthält.

Wiewohl die Verwaltung dieser neuen Datenbestände und die Funktion des zugehörigen Monitors nicht trivial sind, darf festgestellt werden, daß bekannte Methoden zur Verwirklichung ausreichen.

Für das bisher ungelöste Problem der Programm-Authentifikation bietet sich nach den Ausführungen des letzten Abschnitts ein unbekanntes Schreib-Kennwort an. Diese Wahl bietet zwei Vorteile:

- die Authentifikationsinformation ist unfälschbar, da generell unbekannt;
- die Veränderung des Programms kann mit Hilfe der im vorangehenden Abschnitt eingeführten Methoden extrem eingeschränkt werden!¹⁸⁵

Um dieses Schreib-Kennwort als Authentifikation verwenden zu können, wird es in die oben geforderte Liste der berechtigten Programme eingetragen - diese Tatsache wurde in Abbildung 11 vorweggenommen, da die Authentifikations-Information dort in der Programm-Identifikations-Liste bereits als "Soll-Kennwort" bezeichnet wird. Dem Monitor ist es nun möglich, diesen Eintrag mit dem im Katalogeintrag für die Programmdatei zu vergleichen. Um das Programm zu verändern, muß man das Schreib-Kennwort - da unbekannt - auf irgend einem Weg definiert verändern oder löschen. Da die Pro-

¹⁸⁵ Ist die Programmdatei gar keiner Gruppe zugeordnet, so daß der Monitor auch keiner Kennung das Datei-Kennwort verfügbar macht, ist eine Veränderung des Programms sogar nur unter Mitwirkung des Systemverwalters möglich.

gramm-Identifikations-Liste jedoch nicht durch denselben Vorgang modifiziert wird, ist die neue Fassung des Programms solange nicht mehr zugriffsberechtigt, bis eine autorisierte Instanz die Synchronität der beiden Einträge wiederherstellt.

Abb. 12 stellt den Ablauf der Berechtigungsprüfung funktional dar, wobei die im vorangegangenen Abschnitt beschriebene Technik zum Schutz gegen Umgehung des Monitors impliziert wird. Zunächst ist festzuhalten, daß der dargestellte Mechanismus nur dann in Aktion tritt, wenn ein Kennwortfehler beim Eröffnen einer Datei erkannt wird; das Eröffnen einer nicht mehrfachverwendbaren Datei (oder einer, deren Besitzer keiner Gruppe angehört) verläuft unverändert, es sei denn, es fehle ein in einem solchen Fall explizit gefordertes Kennwort. Da es sich in diesem Fall jedoch um einen echten Anwenderfehler handelt, kann der erhöhte Aufwand vertreten werden; in den anderen Fällen ist das Grundprinzip der Anwenderfreundlichkeit gewahrt, weil der von Datenschutzerfordernissen nicht belastete Anwender keinen höheren Aufwand erbringen muß. Erst wenn ein Kennwortfehler erkannt wird, tritt also der Monitor in Funktion:

- als erstes stellt er aus ihm zugänglichen Systemtabellen den Namen der Datei fest, aus der das Programm geladen wurde;
- anschließend prüft er, ob dieses Programm im verarbeitungs-orientierten Teil der Zugriffskontrollliste der angeforderten Datei aufgeführt ist; versagt diese Prüfung, so muß der Zugriffswunsch abgewiesen werden: das Programm konnte *nicht identifiziert* werden;
- bei positiver Identifikation wird nun aus der Programm-Identifikations-Liste das Soll-Kennwort ermittelt und mit dem verglichen, der im konventionellen Katalog für die Datei eingetragen ist, aus der das Programm geladen wurde; sind beide unterschiedlich, wird der Zugriffswunsch an dieser Stelle abgewiesen: das identifizierte Programm konnte *nicht authentifiziert* werden¹⁸⁶;
- erst, wenn das Programm sowohl identifiziert als auch authentifiziert werden konnte, verhilft ihm der Monitor zum Eröffnen der Datei.

Bemerkenswert an der neuen Methode ist vor allem die völlig neuartige und unkonventionelle Rolle, die das Datei-Kenn-

¹⁸⁶ Der Vollständigkeit halber muß hinzugefügt werden, daß Identifikation und Authentifikation entfallen, wenn der verfahrensorientierte Teil der Zugriffs-Kontrollliste das Element "Alle" (s. Abschnitte 3.2 und 3.4.1) enthält; dieser Fall ist jedoch nur im Zusammenhang mit dem in der Abbildung der Klarheit halber nicht explizit dargestellten, umfassenderen Schutz der Gruppenzugehörigkeit mit Hilfe von unbekannten Datei-Kennwörtern von Belang; andernfalls wäre die Information "Alle" durch den Verzicht auf Schutz durch ein unbekanntes Datei-Kennwort ebenso darstellbar.

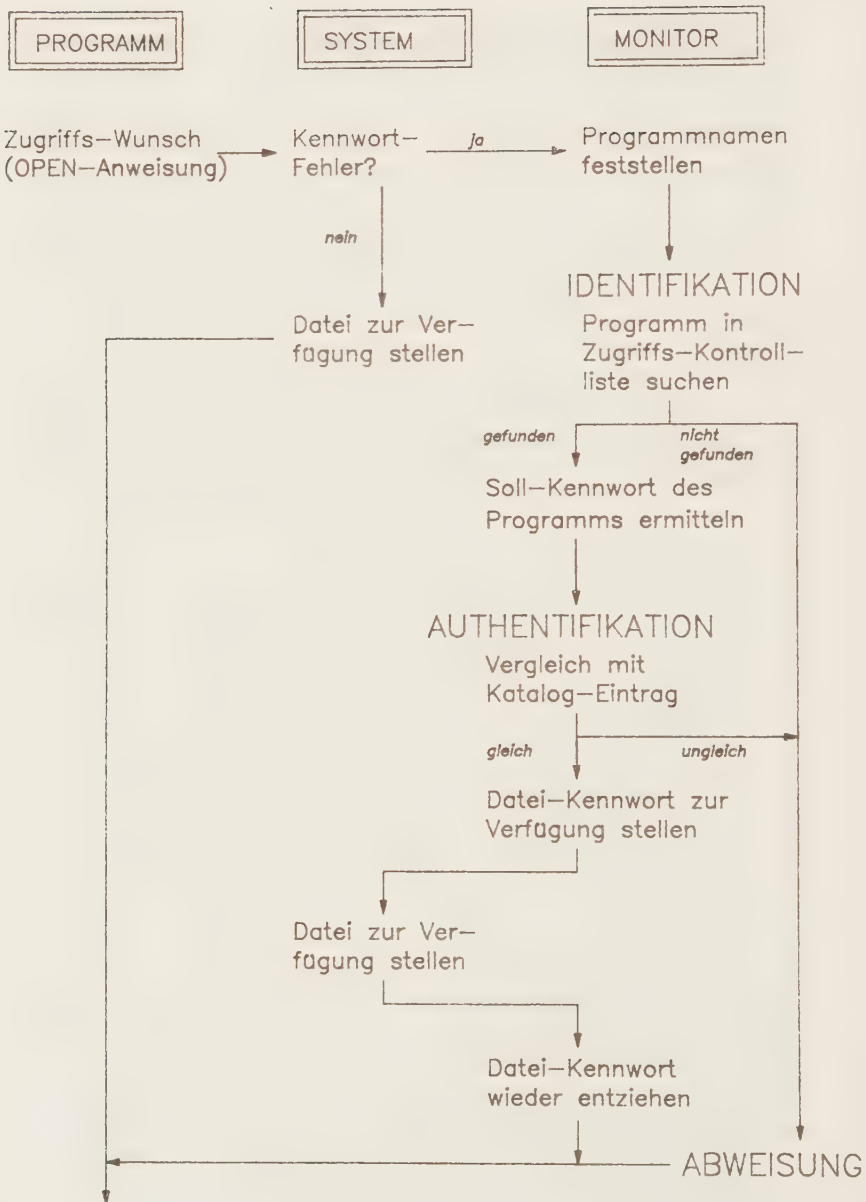


Abb. 12: Realisierung des Verarbeitungsschutzes

wort spielt. Zwar wird auch hier der Zugriff auf die Programmdatei beschränkt, so daß eine unzulässige Veränderung nicht durchgeführt werden kann. Funktional steht jedoch die Authentifikations-Eigenschaft als neue Qualität im Vordergrund; und diese hat überhaupt nichts mehr mit dem Schutz der zugehörigen Datei zu tun:

- zum Zeitpunkt der Authentifikation ist diese bereits (zum Ausführen) geöffnet;
- die Schutzwirkung bezieht sich auf einen völlig unabhängigen Datenbestand (die zu verarbeitende Datei).

Neben der ursprünglichen, "passiven" Aufgabe, als Referenz-Information für einen Ausweis zu dienen, hat der Kennwort-Eintrag im Dateikatalog eine neue, "aktive" Funktion erhalten, indem er selbst als Ausweis dient, um die Identität der Datei zu verifizieren. Diese Doppelfunktion muß als ganz neuartige Erweiterung der Wirkungsweise bezeichnet werden.

Die auffallende Einfachheit der Darstellung der Methodik des Verarbeitungsschutzes entspricht die der technischen Lösung, die gefunden wurde. Es ist wert, die Tatsache hervorzuheben, daß die in Abschnitt 3 dargestellten Schutz-techniken größtenteils an Betriebssystemen mit experimentellem oder wissenschaftlichem Charakter entwickelt wurden (allen voran das berühmte MULTICS). Die hier dargestellte Methode zur Realisierung des Verarbeitungsschutzes - ja der Lösungsansatz selber - ließen sich dagegen - zugegebenermaßen als "Erker" - in einem kommerziellen "all or nothing"-System verwirklichen. Man kann darüber spekulieren, ob es - wie in der Evolution - der Unvollkommenheit als Motivation bedurfte, um eine Weiterentwicklung einzuleiten.

4.4.3 Projektstand

Die vorgestellte Technik wurde für die Praxis entwickelt und ist deshalb auch praktisch erprobt worden. Sowohl die Erweiterung des Objektschutzes in BS2000 durch die Hinzunahme der Gruppenstrukturen mit Hilfe des Prinzips der unbekannten Datei-Kennwörter, als auch die dargestellte Technik des Verarbeitungsschutzes wurden bereits im Jahre 1982 unter dem Projektnamen GSD (Gruppenspezifische Dateien) mit einem Aufwand von ungefähr 9 Mannmonaten realisiert. Diese Implementation kann jedoch nur als eine Zwischenlösung angesehen werden, die zwar einige drängende Probleme löste, im wesentlichen aber dazu diente, die entwickelten Methoden zu überprüfen. Denn, um die erforderlichen Funktionen mit minimalem Aufwand realisieren zu können, wurden alle erstellten Programme und Prozeduren ohne Zuhilfenahme irgendwelcher privilegierter Systemfunktionen realisiert; nur in einem - aus der Perspektive der hier geschilderten Wirkungsweisen eher untergeordneten - Modul wird lesend auf einige Systemtabellen zugegriffen. Dieser Verzicht auf eine Einbettung ins Betriebssystem selbst hat jedoch zur Folge, daß

- eine spezielle Schnittstelle (Unterprogramm-Aufruf) erforderlich war, um gruppen- und verarbeitungs-geschützte Dateien eröffnen zu können,
- zwei Dienstprogramme erforderlich sind zur Verwaltung jeweils der Programm-Identifikations-Liste und der erweiterten Zugriffs-Kontrolllisten,
- der Monitor als eigener Benutzerprozeß mit allen anderen Prozessen um die Systemdienste konkurriert - wenn auch mit höherer Privilegierung.

Vor allem die Notwendigkeit, die Dienste des Monitors mit einer eigenen Schnittstelle anzufordern, hat sich erwartungsgemäß als schweres Hindernis für einen breiten Einsatz von GSD erwiesen. Da die gewöhnliche OPEN-Anweisung ersetzt werden muß,¹⁸⁷ haben Programme, die nicht auf GSD hin implementiert wurden - die neue Schnittstelle also nicht verwenden - keinerlei Zugriffsmöglichkeiten zu derart geschützten Dateien. Nur solche Datenbestände dürfen mit GSD geschützt werden, auf die keine Dienstprogramme (einschließlich der wichtigen Sortierfunktion) und keine früher erstellten Anwenderprogramme zugreifen müssen. Der Einsatz von GSD bleibt deshalb auf wenige, sensitive Dateien beschränkt.

Da sich die Methodik selbst als wirksam erwiesen hatte, ist beschlossen worden, den dringend erforderlichen, umfassenden Schutz zu realisieren, indem eine tiefere Verflechtung mit dem Betriebssystem eingegangen wird. Derzeit wird das neue Projekt GBS2 (Gruppenstrukturen in BS2000) mit diesem Ziel vorangetrieben. Es sieht eine volle Integration aller dargestellten Funktionen in die Betriebssystemebene vor und zeichnet sich durch folgende Eigenschaften aus:

- die OPEN-Funktion des Datenverwaltungssystems selbst wird erweitert; hierdurch ist die Wirkung unabhängig davon, wann und von wem Programme erstellt wurden;
- Alle Steuerungs- und Kontroll-Funktionen werden auf der Ebene der Kommandosprache des Systems verwirklicht:
 - funktionale Erweiterung vorhandener Kommandos (z.B. FILE und CATALOG zur Verwaltung der Katalog-Erweiterungen, FSTATUS zur Statusabfrage für sogenannte "Gruppendateien"),
 - Bereitstellen neuer Kommandos (z.B. GROUP zur Verwaltung der Gruppenstrukturen, PROGDEF zur Verwaltung der Programm-Identifikations-Liste, GSTATUS zur Abfrage der eigenen Gruppen-Umgebung),
 - Implikationen (das vorhandene SEVER-Kommando veranlaßt nunmehr auch eine Löschung der entfernten Benutzererkennung aus der Gruppenstruktur).

¹⁸⁷ Die Portabilität solcher Programme wird gewahrt, indem das Schnittstellen-Unterprogramm an Hand einer systemweiten Anzeige erkennen kann, ob die aktuelle Systemumgebung GSD kennt; wenn nicht, wird lediglich ein gewöhnlicher OPEN-Aufruf ausgeführt.

Beibehalten wird, daß die Anwender, die keiner Gruppe angeschlossen sind oder keine mehrfachverwendbare Dateien verwenden (z.B. Software-Entwickler, testende Programmierer, Wissenschaftler mit nicht-personenbezogenen Daten¹⁸⁸) GBS2-Monitor nicht zum Zugriff durchlaufen müssen, d.h. nicht belastet werden; dies ist, wie in Abschnitt 2.1.1 ausgeführt, eine Grundbedingung für die Akzeptanz eines Sicherheitssystems.

Für das Projekt GBS2 wurde im Sinne der ADV-Richtlinien ein detailliertes fachliches Feinkonzept erarbeitet und mit den betroffenen Mitarbeitern abgeglichen. Derzeit ist die Implementierung mit projektbegleitender Dokumentation in vollem Gange und soll noch im laufenden Jahr (1985) in einer ersten Version abgeschlossen werden.

4.4.4 Abschätzung des Sicherheitsgewinns

4.4.4.1 Praktische Erfahrungen

Es ist recht fragwürdig, praktische Erfahrungen heranzuziehen, um den Sicherheitsgewinn einer Datenschutz-Maßnahme abzuschätzen:

- es liegt i. allg. in der Natur der Sache, daß versucht wird, erfolgreiche, subversive Angriffe zu verheimlichen;⁸⁹
- eigene Versuche, das Verfahren zu überlisten, leiden aller Voraussicht nach unter den "blinden Flecken", die sich nach langer Beschäftigung mit einer speziellen Materie einstellen können; sie können - wie ein Programmtest - höchstens Lücken aufdecken, niemals aber die durchgehende Sicherheit nachweisen.

Nur in einer Situation können praktische Erfahrungen deshalb zu bewertbaren Aussagen herangezogen werden: beim *versehentlichen* Auslösen der Schutzmechanismen wird meist eine - unberechtigte - Fehlermeldung durch den noch unerfahrenen Anwender abgegeben. Das Ausbleiben solcher Meldungen kann geradezu als ein Alarmzeichen gewertet werden; denn der Umgang mit einer neuen Eigenschaft des Systems oder seiner unmittelbaren Umgebung ist selten leicht und fehlerfrei zu erlernen. In der Anfangsphase des Einsatzes von GSD wurde der Verfasser jedoch mehrfach und von allen betroffenen Mitarbeitern um Hilfe gebeten:

- in den meisten Fällen war der Versuch gescheitert, geschützte Daten durch ein (versehentlich) nicht zugelassenes Programm zu verarbeiten; die Programm-Identi-

¹⁸⁸ Selbstredend können auch solche Anwender die Dienste des GBS2 anfordern, wenn dies aus anderen Gründen (z.B. Plagiat-Schutz) wünschenswert erscheint.

¹⁸⁹ Es gibt Fachleute, die darauf spezialisiert sind, Sicherheitslücken aufzudecken, doch dürfte ihr Einsatz der hohen Kosten wegen eher im militärischen oder kommerziellen Bereich in Frage kommen.

fikations-Liste mußte ergänzt werden;

- in einem Fall war ein Objektmodul durch ein neues ersetzt worden, ohne daß die vorgesehenen Änderungsverfahren durchgeführt wurden: es war dies ein typischer Fall des "Versions-Problems".¹⁹⁰

Die praktische Erfahrung zeigt somit, daß das beschriebene Verfahren einen zuverlässigen Schutz gegen unbeabsichtigten Bruch des Verarbeitungsschutzes bietet.

4.4.4.2 Sicherheit des Monitors

Es wurde bereits mehrfach erwähnt, daß ein System nur dann als sicher angesehen werden kann, wenn kein Monitor, der eine Schutzfunktion verwirklicht, umgangen werden kann. Dies könnte auf mehrererlei Weisen geschehen:

- es gelingt dem Angreifer, dem System vorzutäuschen, er sei der Systemverwalter;
- der Angreifer findet einen Weg, seine Kennung (bzw. eine Kennung, in die er eindringen konnte) in den privilegierten System-Status zu versetzen;
- der Schutzmechanismus des Monitors kann außer Kraft gesetzt werden.

Es sollte als Selbstverständlichkeit gelten, daß die Benutzererkennung des Systemverwalters mit allen denkbaren Mitteln vor Mißbrauch geschützt werden muß. Hierzu gehören nicht nur sorgfältige Wahl und häufiger Wechsel des Passworts, sondern auch eine Begrenzung der für diesen speziellen Benutzer zugelassenen Datenendgeräte und eine extrem restriktive Begrenzung des berechtigten Personenkreises.

Da keines der gängigen Betriebssysteme nuklearisiert ist, muß damit gerechnet werden, daß es i. allg. Wege gibt, unerlaubt in den System-Status zu gelangen. Bei BS2000 war ein solcher Weg in einer früheren Version bekannt. Die Tatsache, daß dem Verfasser derzeit keine solche Methode bekannt ist, darf nicht zu einem falschen Sicherheitsgefühl verleiten. Die Hersteller von Betriebssystemen bleiben aufgefordert, alle Schutzmaßnahmen zu systematisieren und nachprüfbar zu machen. Im Fall der medizinischen Datenverarbeitung darf allerdings bezweifelt werden, daß die hohen Kosten, die einem Angreifer entstehen, wenn solche Schwachstellen systematisch gesucht werden, in einem vernünftigen Verhältnis zum Wert der Daten stehen.

In Abschnitt 4.4.1.2 wurde bereits darauf hingewiesen, daß das Prinzip der unbekannten Datei-Kennwörter die Eigenschaft hat, beim Versagen des Monitors die geschützten Daten erst recht unzugänglich zu machen. Der Monitor kann

¹⁹⁰ S. Abschnitt 2.3.2.5.

folglich nur außer Kraft gesetzt werden, wenn der Angreifer das Kennwort selbst in Erfahrung bringen kann, da dann ein unmittelbarer Zugriff möglich ist. Unter der Voraussetzung, daß der Kennwortgenerator zuverlässig gleichverteilte Werte erzeugt, entfallen alle bekannten "Rate-Verfahren";¹⁹¹ wie sie häufig zum Angriff auf den Benutzerschutz verwendet werden. Dagegen führt die Offenlegung des Kennworts - z.B. in einem Speicherauszug - direkt zum Ziel; das Prinzip der unbekannten Datei-Kennwörter ist deshalb nur wirksam, wenn die Kennwörter intern verschlüsselt werden. Unter diesen Umständen aber verbleiben dem Angreifer nur "brute force"-Methoden, um ans Ziel zu gelangen; im Mittel muß er die Hälfte aller möglichen Werte durchprobieren, bis ihm ein Durchbruch gelingt.

Um eine Vorstellung vom hierzu erforderlichen Aufwand zu gewinnen, wurden drei Experimente an einer DV-Anlage mit einer Nennleistung von ca. 1,5 Mips¹⁹² durchgeführt. In allen Fällen wurden 50.000 von einem Zufallsgenerator erzeugte Werte verwendet, um die mittleren Zeiten zu ermitteln sowie die Streuung der Mittelwerte aus je 1.000 Messungen. Fremdeinflüsse wurden dadurch weitgehend vermieden, daß die Versuche in betriebsarmen Zeiten bei praktisch unbelasteter DV-Anlage durchgeführt wurden: aus der Sicht des Angreifers stellen die Ergebnisse Optimalwerte dar.

Bei dem ersten Experiment wurde angenommen, daß dem Angreifer keinerlei Information über das gesuchte Kennwort vorliegt: er ist gezwungen, bei jedem Versuch ein Kennwort anzugeben und anschließend zu versuchen, das eigentliche Kennwort zu löschen.¹⁹³ Die Messungen ergaben folgende Werte:

- mittlere CPU-Zeit: 3,52 msec (Streuung 0,01 msec),
- mittlere Verweilzeit: 9,58 msec (Streuung 0,22 msec).

Bei 2³² möglichen Werten des 4 Bytes langen Kennworts ergibt dies eine Brutto-Verweilzeit von 238 Tagen bis zum Erfolg unter Aufwendung von 7,6 Millionen CPU-Sekunden.

Das zweite Experiment ging davon aus, daß der Angreifer das Kennwort in seiner verschlüsselten Form in Erfahrung bringen konnte (s.o.). In diesem Fall braucht er seine Versuchswerte lediglich durch die vorhandene Routine verschlüsseln zu lassen und das Ergebnis mit dem gesuchten Wert zu vergleichen. In diesem Fall ergaben die Messungen:

- mittlere CPU-Zeit: 0,97 msec (Streuung 0,02 msec),
- mittlere Verweilzeit: 1,01 msec (Streuung 0,05 msec).

¹⁹¹ Hierzu gehört u.a. das Ausprobieren von Daten aus dem persönlichen Umfeld des berechtigten Benutzers ebenso, wie eine Eingrenzung des betrachteten Wertebereichs auf Phoneme, Dezimalziffern usw.

¹⁹² Mega-Instruktionen pro Sekunde.

¹⁹³ Dieses Verfahren ist wesentlich schneller als der Versuch, die Datei sofort zu eröffnen; im verwendeten Betriebssystem residiert der Katalog im virtuellen Speicher, so daß Ein-/Ausgabe-Operationen lediglich für das Paging erforderlich werden.

Der Angreifer muß folglich mit einer Brutto-Verweilzeit von 25 Tagen und einem Aufwand von 2,1 Millionen CPU-Sekunden rechnen, um das gewünschte Ergebnis zu erlangen.

Der Angreifer könnte sehr schnell zum Ziel kommen, wenn er über eine Entschlüsselungstabelle verfügte. Im dritten Versuch wurde deshalb eine ISAM-Datei erzeugt, deren ISAM-keys jeweils die 28 höherwertigen Stellen der verschlüsselten Werte darstellen, und deren Datenteil die 16 zugeordneten unverschlüsselten Kennwörter enthält. Je Eintrag wurden folgende Zeiten gemessen:

- mittlere CPU-Zeit: 5,53 msec (Streuung 0,02 msec),
- mittlere Verweilzeit: 68,7 msec (Streuung 0,4 msec).

Der hohe Dehnfaktor zwischen CPU- und Verweilzeit, der durch die Ein-Ausgabe-Intensität des Verfahrens bedingt ist, legt es hier nahe, die Aufgabe zu teilen, und etwa 8 Prozesse gleichzeitig ablaufen zu lassen. Auch mit dieser Zeitoptimierung müßte ein Angreifer jedoch eine Brutto-Verweilzeit von ca. 426 Tagen aufbringen und würde 23,8 Millionen CPU-Sekunden verbrauchen¹⁹⁴ - allerdings auf eigener DVA. Hinzu kommt in diesem Fall eine Direktzugriffs-Speicherkapazität von fast 20 GByte.

Während das zuletzt beschriebene Verfahren offensichtlich aus Kostengründen außer acht gelassen werden kann, stellt das zweite eine echte Bedrohung dar, zumal

- eine Leistungssteigerung um einen Faktor von mehreren 100 bei künftigen DV-Anlagen eher wahrscheinlich ist, und
- die erforderliche Verarbeitung nicht auf dem Rechner erfolgen muß, der die bedrohten Daten verwaltet.

Es wäre deshalb sehr wünschenswert, die Datei-Kennwörter in BS2000 künftig - wie dies bereits bei den Passwörtern der Fall ist - in einer Länge von 8 Bytes definieren zu können; hierdurch würden alle Angriffsmethoden der geschilderten Art langfristig wirkungslos gemacht.

4.4.4.3 Grundsätzliche Schwachstellen, Ausblicke

Wie bei allen technischen Gebilden hat auch die vorgestellte Technik zur Realisierung des Verarbeitungsschutzes einige grundsätzliche Schwachstellen, und es ist wichtig, diese offenzulegen, damit

- der Anwender sich durch andere Maßnahmen dagegen schützen kann¹⁹⁵ und
- nach Verbesserungen gesucht werden kann, um den Sicherheitsgrad zu erhöhen.

¹⁸⁴ Bei dieser Vorgehensweise müssen natürlich alle Möglichkeiten berechnet werden, so daß der statistische Faktor 0,5 entfällt.

¹⁹⁵ S. Abschnitt 1.

Zweifellos ist es ein Mangel des in Abschnitt 4.4.1.2 dargestellten Verfahrens zum verbesserten Objektschutz, daß es bisher lediglich Dateien als Objekte schützt; für eine spätere Version wird eine Ausdehnung auf andere Daten und vor allem auf Datenkanäle wie das DCAM¹⁹⁶ und die Interprozeß-Kommunikation vorgesehen.

In Bezug auf den Verarbeitungsschutz sind zwei Schwachstellen bisher aufgefallen. Beide hängen damit zusammen, daß die Funktion eines identifizierten und authentifizierten Programms von außen beeinflußt werden kann.

a) Dynamisches Binden:

Sofern ein identifiziertes und authentifiziertes Programm zur Objektzeit Module aus anderen Dateien nachlädt, bieten diese natürlich eine Möglichkeit, subversive Funktionen in den Ablauf einzuschleusen. Es ist in der Praxis nicht möglich, einen Schutz gegen diese Bedrohung in das vorgestellte Konzept einzubringen; denn:

- der Prüfungsvorgang kann bereits abgeschlossen sein, wenn der Nachladevorgang ausgeführt wird,
- es gibt derzeit keinen Weg, bei der Prüfung der Zugriffsberechtigung festzustellen, welche Teile des aktiven Programms vorher dynamisch nachgeladen wurden.

Um das dynamische Einschleusen von "Trojanischen Pferden" und "Falltüren" zu verhindern, gibt es nach augenblicklicher Erkenntnislage nur die Möglichkeiten

- das dynamische Nachladen in identifizierten und authentifizierten Programmen zu verbieten - eine Forderung, die in Hinblick auf die vielen, zur Objektzeit einzubindenden Hilfsfunktionen des Betriebssystems und systemnaher Softwareprodukte als unrealistisch bezeichnet werden muß¹⁹⁷ oder
- das dynamische Binden in solchen Programmumgebungen nur aus geschützten Subsystemen zuzulassen, die wiederum durch die beschriebenen Mechanismen gegen Veränderung geschützt werden könnten.

Angesichts der letztgenannten Lösungsmöglichkeit muß es als außerordentlich bedauerlich angesehen werden, daß der bisher zumindest rudimentär gebotene Ringschutz des BS2000 nicht ausgebaut wird, sondern statt dessen aus offensichtlich marktpolitischen Motiven gekündigt wurde.

¹⁹⁶ Data Communications Access Method; das Problem liegt hier und in einigen weiteren, ähnlich gelagerten Fällen darin, daß diese Betriebsmittel keine direkte Zuordnung zu einer "besitzenden" Benutzerkennung aufweisen.

¹⁹⁷ Dagegen wäre die Forderung, aus pragmatischen Gründen Programme, die mit Hilfe einer Identifikations-Liste authentifiziert werden sollen, nur statisch zu binden, durchaus akzeptabel.

b) Interaktive Diagnose-Hilfsmittel:

Fast alle modernen Betriebssysteme bieten dem Anwender die Möglichkeit, ein Programm interaktiv zu testen. Die hierzu bereitgestellten Funktionen beschränken sich nicht darauf, Programme an definierten Stellen anhalten zu lassen, um den Speicherinhalt in der vorliegenden Situation analysieren zu können, oder das Programm schrittweise in seiner Funktion zu verfolgen ("trace"); vielmehr erlauben sie auch, funktionale Korrekturen zur Objektzeit anzubringen. Es können

- die Werte der im Hauptspeicher oder in den Registern des Rechners gespeicherten Daten verändert werden,
- Teile des Programms selbst im Hauptspeicher modifiziert werden, wodurch andere - meist verbesserte - Arbeitsweisen entstehen,
- Befehlszähler und andere dem Verarbeitungsrechner eigene Anzeigen manipuliert werden.

Diese Fähigkeiten der interaktiven Testhilfen sind nicht generell auf den Testfall beschränkt, bei dem auf keine schutzwürdigen Daten zugegriffen werden sollte; sie stellen deshalb eine schwerwiegende Bedrohung des Verarbeitungsschutzes dar, indem unerwünschte Funktionsweisen eingeschleust werden können, ohne daß die vorgesehenen Schutzmaßnahmen dies erkennen können.

Dieser Gefahr könnte relativ leicht auf der Betriebssystem-Ebene begegnet werden, wenn ein ggf. vorhandenes Schreib-Kennwort für das Lademodul des Programms angegeben werden müßte, um mit Diagnose-Hilfsmitteln schreibend im Hauptspeicher u. dergl. eingreifen zu dürfen. Eine solche Einschränkung würde sich offensichtlich auch organisch in die geschilderten Mechanismen des Verarbeitungsschutzes einfügen.

4.5 Systemverwalter, Datenschutzbeauftragter

Das Thema Verarbeitungsschutz, das sich ja damit befaßt, die mißbräuchliche Verwendung der Datenverarbeitung durch zugriffsberechtigte Anwender zu verhindern, kann nicht abgeschlossen werden, ohne daß auf die Problematik der Sonderstellung des Systemverwalters hingewiesen würde. Man muß klar erkennen, daß auch die Technik des Verarbeitungsschutzes nicht ohne einen Verantwortlichen auskommt, der u.a. bestimmt, welche Programme auf die zu schützenden Daten jeweils wirken dürfen, bzw. die Programme mit einer Authentifikations-Information legitimiert. Ebenso wichtig ist aber die Erkenntnis, daß diese Vertrauensperson hierfür keinerlei programmiertechnischen Kenntnisse zu haben braucht, sofern nur eine unabhängige Revisionsinstanz die Korrektheit der Verarbeitungsfunktion bestätigt. Dieses Denkmodell ist jedoch vorerst reine Theorie; die Schwierigkeit ist darin zu sehen, daß es nach der Struktur aller bekannten Betriebssysteme eine Person geben muß, die "alles

kann"; vor allem ist diese "Systemverwalter" genannte Person in der Lage

- Passwörter und Datei-Kennwörter zu ändern oder zu löschen, ohne ihren aktuellen Wert angeben zu müssen,
- in beliebige Systemtabellen - einschließlich Zugriffs-Kontrolllisten - verändernd einzugreifen,
- Module mit praktisch beliebiger Funktion zu entwickeln und in das Betriebssystem einzubringen.¹⁹⁸

Dies alles bedeutet eine erhebliche Bedrohung des Datenschutzes im allgemeinen und des Verarbeitungsschutzes im besonderen, es sei denn, der Systemverwalter übernimmt die Funktion des Datenschutzbeauftragten der Installation in Personalunion - eine nicht unangreifbare Konstruktion, wenn man das Grundziel des Verarbeitungsschutzes betrachtet, von der doppelten Arbeitsbelastung und Verantwortung abgesehen.

Wünschenswert wäre es deshalb, diese beiden Funktionsbereiche mit völlig disjunkten Befugnissen nebeneinander führen zu können:

- der Systemverwalter behält alle Möglichkeiten mit Ausnahme des Eingriffs in datenschutzrelevante Bereiche wie Pass- und Kennwörter, Zugriffs-Kontrolllisten usw. aber auch die einschlägigen Systemfunktionen;
- der Datenschutzbeauftragte erhält ausschließliche, vom Systemverwalter unabhängige Verfügungsgewalt über die Datenstrukturen, die die Zugriffsberechtigung regeln; die zugehörige, spezielle Benutzererkennung erhält darüber hinaus keinerlei Befugnisse, vor allem nicht die, Programme zu erstellen oder Daten in fremde oder aus fremden Kennungen zu übertragen.

Bei der derzeitigen Struktur praktisch aller Betriebssysteme muß diese Forderung als utopisch angesehen werden; denn stets gibt es einen maximalprivilegierten Systemzustand, von dem aus alle Benutzer ihre Befugnisse direkt oder indirekt übertragen bekommen. Diese höchste Ebene ist deshalb erforderlich, weil es bei den großen, praktisch nicht vollständig austestbaren Betriebssystemen stets erforderlich ist, bei Fehlern oder instabilen Zuständen einzugreifen, und weil dies in den allermeisten Fällen nur mit Hilfe einer solchen Globalbefugnis möglich ist.

Um die Forderung nach disjunkten Funktionsbereichen für die beiden wichtigsten Aufgabengebiete in einer datenschutzsensitiven Umgebung erfüllen zu können, wäre eine beiden überstellte hierarchische Funktionsebene geeignet, deren besonders privilegierter Befehlsvorrat also nicht einmal dem Systemverwalter verfügbar wäre, und deren Bedienung dem Datenschutzbeauftragten alleinbestimmend (z.B. über eine besonders geschützte Benutzererkennung, wie oben beschrieben)

¹⁹⁸ Hierauf beruht natürlich auch die dargestellte Verwirklichung des Verarbeitungsschutzes!

vorbehalten ist. Darüber hinaus dürfte der Datenschutzbeauftragte - wie dargestellt - keinerlei weiteren Befugnisse haben, weder zum Eingriff in das System noch zur eigenverantwortlichen Verarbeitung.

Die praktischen Konsequenzen aus diesen Forderungen aber sind:

- daß das betreffende Betriebssystem "nuklearisiert" wird,¹⁹⁹ wobei der Systemkern mit den dem Systemverwalter verfügbaren Befehlen nicht ansprechbar ist.
- daß dieser Kern völlig fehlerfrei realisiert wird, um die Notwendigkeit eines irgendwie gearteten Eingriffs in seine Funktion zu eliminieren, und um die datenschutzrelevanten Funktionen absolut zu gewährleisten.

Vorstellbar wäre es, diesen Sicherheitskern einschließlich der dem Datenschutzbeauftragten vorbehaltenen Kommando-oberfläche in Firmware zu realisieren.

Es ist aus all diesen Gründen dringend zu wünschen, daß die von Bates 3 geforderte strategische Vorgehensweise²⁰⁰ zum Ausgangspunkt neuer Bestrebungen gemacht wird, die Systemstrukturen im Sinne von Datenschutz und Datensicherheit zu verbessern. In Anbetracht der voraussichtlichen Schwierigkeiten und Kosten für eine solche Entwicklung stimmt eine realistische Abschätzung der Wahrscheinlichkeit, daß solche Techniken in absehbarer Zeit in kommerziell vertriebene Betriebssysteme Eingang finden, weniger optimistisch.

¹⁹⁹ S. Abschnitt 3.1.

²⁰⁰ S. Abschnitt 1.

5. ZUSAMMENFASSUNG

Die Notwendigkeit von Datenschutz und Datensicherheit stehen außer Zweifel; ja sie erhalten einen steigenden Stellenwert dadurch, daß immer mehr Menschen den Umgang mit der Datenverarbeitung erlernen und somit auch zu Gefahrenquellen werden können. Hinzu kommt, daß das allgemeine Bewußtsein der Bevölkerung durch gesellschaftliche Strömungen geschärft worden ist, und der sorgfältigere Umgang mit gespeicherten Informationen daher eine Grundvoraussetzung geworden ist, um sinnvolle und verantwortungsbewußte Datenverarbeitung betreiben zu können. Besonders gilt dies im Bereich der personenbezogenen Daten, da sie - im Gegensatz zu technischen, wirtschaftlichen, militärischen Informationen usw. - "Objekte" beschreiben, die im allgemeinen selbst nicht dem Besitzer der Daten "verfügbar" sein sollen. Unter den personenbezogenen Daten müssen die ärztlichen als besonders sensitiv angesehen werden.

In Bezug auf die Methoden unterscheidet sich der Datenschutz im medizinischen Bereich keineswegs vom Schutz anderer personenbezogener Daten. Die Sensitivität und Intimität der Daten einerseits und die bewährte Tradition der Schweigepflicht andererseits, die eine wesentliche, weil vertrauensbildende Grundlage ärztlichen Handelns darstellt, geben dem Datenschutz in diesem Bereich eine herausragende Bedeutung. Hinzu kommt ein gerade bei der vorliegenden Arbeit signifikanter Aspekt, daß die medizinische Datenverarbeitung in großem Umfang auch "anonymisierte" Daten verwendet - so beispielsweise in der Epidemiologie, bei statistischen Querschnittsuntersuchungen und dergleichen. Das mangelnde Bewußtsein, daß solche anonymisierten Daten (nicht zu verwechseln mit statistischen Größen, die aus den ggf. anonymisierten Daten gewonnen werden) fast immer "entanonymisiert" werden können, führt dazu, daß mit solchen Informationen manchmal sorgloser umgegangen wird, als geboten.

Datenschutz und Datensicherheit werden u.a. durch juridische, bauliche, organisatorische, personalpolitische und DV-technische Mittel erreicht, und es bedarf eines Zusammenwirkens dieser Komponenten, um einen möglichst guten Schutz zu erreichen - im Rahmen eines vernünftigen Kosten/Nutzen-Verhältnisses. Man kann jedoch feststellen, daß dort, wo die persönliche, verantwortete Entscheidung einer menschlichen Instanz nicht zwingend ist, einer technischen Absicherung gegenüber anderen Methoden der Vorzug zu geben ist, die immer wieder durch menschliches Fehlverhalten, gleich welcher Ursache - gefährdet sind. Jede technische Schutzmaßnahme, die z.B. eine organisatorische ersetzt, ist als Sicherheitsgewinn zu betrachten. Es ist deshalb legitim, nach wirkungsvollen technischen - speziell DV-technischen - Schutzmethoden zu suchen, solange man nicht übersieht, daß sie allein keine vollständige Lösung des Problems bieten können.

Die Gefährdungen, denen schutzwürdige Daten ausgesetzt sind, lassen sich in fünf Klassen einteilen:

- Zerstörung von Daten, Geräten oder Infrastruktur,
- Datendiebstahl (einschließlich "passiver" Abhörmethoden),
- unberechtigte Systembenutzung,
- unberechtigter/unbeabsichtigter Datenzugriff und
- unberechtigte Verarbeitung.

Es läßt sich leicht zeigen, daß den ersten beiden Kategorien nicht oder nur unzureichend mit DV-technischen Maßnahmen begegnet werden kann; hier sind vor allem bauliche und organisatorische Lösungen erforderlich.

Die dritte Gefahrenklasse ist gründlich untersucht worden, und hier stehen mächtige Methoden zur Verfügung, auch wenn sie nicht immer im erforderlichen Maße eingesetzt werden.

Die Bewältigung der vierten Gefährdung läßt sich als Lösung des Problems der "kontrollierten Mehrfachverwendung" von Daten identifizieren; die betroffenen Daten sollen zwar einer Mehrzahl von Anwendern (ggf. mit unterschiedlichen Einschränkungen wie "nur lesen", "nur anfügen" o.ä.) verfügbar sein, aber auch nur diesen. Auch diese Fragestellung kann grundsätzlich als gelöst angesehen werden.

Anders verhält es sich bei der fünften Klasse. Die Problemstellung selbst ist subtilerer Natur: es handelt sich darum, zu verhindern, daß ein zugriffsberechtigter Anwender seine rechtmäßigen Befugnisse mißbraucht, indem er unstatthafte Verarbeitungsfunktionen (Übertragung an unbefugte Dritte, gezielte, subversive Veränderung der Daten usw.) ausführt. Trotz eines wachsenden Problembewußtseins sind auf diesem Gebiet bislang nur Teillösungen (z.B. gegen Verrat durch Geheimnisträger) und pragmatische Insellösungen (z.B. in Bezug auf umfangreiche Datenbanksysteme) bekannt geworden.

Es ist das Hauptziel der vorliegenden Arbeit, eine geschlossene und allgemeine Theorie der Verhinderung der unberechtigten Verarbeitung zu bieten, und von einer technischen Lösung hierzu zu berichten. Sowohl die angegebene Systematik als auch die Realisierung sollen mit dem Begriff

Verarbeitungsschutz

bezeichnet werden. Es darf behauptet werden, daß damit eine neue Qualität in den Datenschutz hineingetragen wird.

Eine der Grundlagen der bisherigen Arbeiten über Datenschutz ist die sogenannte "Zugriffsmatrix", ein gedachtes Gebilde, das die Subjekt/Objekt-Beziehung zwischen Anwendern und Daten verkörpert, wobei die Matrixpunkte die jeweiligen Befugnisse dokumentieren. Die Funktionsfähigkeit

der Schutzmaßnahmen, die durch diese zweidimensionale Beziehung dargestellt werden, wird - neben der fehlerfreien Realisierung der entsprechenden Systemsoftware - durch die Gewißheit bestimmt, mit der die einzelnen Subjekte als berechnete Anwender festgestellt werden können (Schutz gegen unberechtigte Systembenutzung, s.o.). Allen Verfahren, die den berechtigten vom unberechtigten Anwender unterscheiden sollen, ist gemeinsam, daß sie zwei getrennte Informationen benötigen, die sie auf ihre gegenseitige Zugehörigkeit prüfen müssen:

- eine *Identifikation*, die das Subjekt kennzeichnet (benennt), und
- eine *Authentifikation*, die dazu dient, die vorgebliche Identität des Subjekts zu verifizieren.

Als Authentifikationsmittel dienen typischerweise geheime Passwörter, maschinell lesbare Ausweise und dergleichen.

Die Problemstellung des Verarbeitungsschutzes setzt jedoch bereits voraus, daß die handelnden Subjekte zugriffsberechtigt sind, d.h. daß sie identifiziert und authentifiziert wurden, und daß die Schnittstelle der Zugriffsmatrix, die ihre Beziehung zu einem Objekt festlegt, Befugnisse enthält. Im Blickpunkt steht hier vielmehr die Frage, ob nicht ein solches Subjekt ein unzulässiges, weil schädliches Verfahren anwendet. Die Gefahrenquellen sind in dieser weiterführenden Sicht die Programme, die das berechnete Subjekt verwendet. Das Ziel des Verarbeitungsschutzes ist es, schutzwürdige Daten auch von berechtigten Anwendern nur mit definierten Verfahren verarbeiten zu lassen.

Die daraus folgende Erkenntnis ist einfach, wurde jedoch bisher nicht formuliert: die Zugriffsmatrix muß um eine Dimension erweitert werden; das Verfahren tritt als aktive Komponente hinzu. Diese neue, erweiterte Sicht der Grundstruktur des Zugriffsschutzes stellt die Grundlage für das allgemeine Konzept des Verarbeitungsschutzes dar.

Die Dualität der aktiven Komponenten der nunmehr dreidimensionalen Zugriffsmatrix veranschaulicht, daß es nicht ausreicht, allein den Anwender in seiner Identität zweifelsfrei zu bestätigen. Es muß vielmehr auch das anzuwendende Verfahren eindeutig bestimmbar sein. Es ist üblich, einem Programm einen Namen zu geben, und die aktive Programmausprägung kann durch den Namen der Datei gekennzeichnet werden, aus der sie geladen wurde. Die Analogie zum Schutz gegen unberechtigte Systembenutzung führt jedoch zu der völlig neuartigen Forderung nach einer *Programm-Authentifikation*. Hierdurch allein erhält das Konzept der dreidimensionalen Zugriffsmatrix eine über das Schematische hinausweisende, praktische Funktionalität.

Zur Realisierung des Verarbeitungsschutzes sind somit zwei Probleme zu lösen:

- die Abbildung der abstrakten, dreidimensionalen Zu-

griffsmatrix in praktisch handhabbare Strukturen und

- die Definition und Implementation eines Mechanismus zur Identifikation und Authentifikation für Programme.

Beide Aufgabenkomplexe haben sich in Form einer Erweiterung des Betriebssystems BS2000 von Siemens bewältigen lassen.

Eine der bekannten Techniken zur Reduktion der zweidimensionalen Zugriffsmatrix auf praktisch einsetzbare Datenstrukturen ist es, den zu schützenden Datenbeständen "Zugriffs-Kontrolllisten" beizuordnen. Diese stellen eine Aufzählung der zugriffsberechtigten Anwender jeweils mit ihren individuellen Befugnissen dar. Oft werden sie durch die Bildung von Anwendergruppen komprimiert. Beachtet man nun, daß die Dateien, in denen die Programme ladefähig gespeichert sind, ganz normale Objekte sind, so erkennt man, daß man ihre Zugriffs-Kontrolllisten benutzen kann um die Befugnis-Beziehung zwischen Subjekten und Verfahren abzubilden. Für die Realisierung der Berechtigungsbeziehung zwischen Objekten und Verfahren dagegen ist eine neue Informationsstruktur erforderlich. Offensichtlich ist den zu schützenden Datenbeständen eine zweite Zugriffs-Kontrollliste zuzuordnen, die die verarbeitungsberechtigten Programme benennt.

Diese zweite Zugriffs-Kontrollliste wurde in einer Erweiterungsdatei zum Systemkatalog realisiert. Diese enthält nur Einträge für Dateien, die dem Verarbeitungsschutz unterliegen sollen; sie wird durch neue, privilegierte Parameter des CATALOG-Kommandos gepflegt.

Zur Identifikation der Programm wurde eine neue Datei eingerichtet, die jeweils Programmnamen mit den Bezeichnungen der Dateien verknüpft, in denen jene als Lademodule abgelegt sind. Das wesentlich schwierigere Problem der Programm-Authentifikation konnte durch die Weiterentwicklung einer bereits vor Jahren vom Verfasser erstmals entwickelten Technik gelöst werden, die als Technik der unbekannten Datei-Kennwörter bezeichnet wird.

Diese Technik der unbekannten Datei-Kennwörter erlaubt es, Befugnisbeziehungen herzustellen und zu kontrollieren, die vom Betriebssystem nicht vorgesehen sind. Speziell zur Programm-Authentifikation wird jeder Lademodul-Datei, die - bezogen auf einen oder mehrere Datenbestände - ein verarbeitungsberechtigtes Programm enthält, und somit einen Eintrag in die Programm-Identifikations-Datei erhält, ein von einem Zufallszahlengenerator erzeugtes, nach außen unbekanntes Schreib-Kennwort zugewiesen, das auch in die Programm-Identifikations-Liste eingetragen wird. Hierdurch werden zwei Wirkungen erzielt:

- beim Eröffnen eines geschützten Datenbestandes kann im Zuge der Programm-Identifikation das "Soll-Kennwort" ermittelt werden und mit dem Eintrag im herkömmliche Dateikatalog verglichen werden; nur bei Übereinstimmung ist das Programm authentifiziert und darf die Daten verarbeiten;

- um eine Programm-Änderung durchzuführen, muß das Kennwort - da unbekannt - von einem besonders privilegierten Mitarbeiter entfernt werden; damit erlischt aber die Authentifizierbarkeit, bis die neue Version durch einen speziell beauftragten Mitarbeiter mit Hilfe eines ihm vorbehaltenen Kommandos beglaubigt wird.

Durch diese völlig neuartige Verwendungsart der Datei-Kennwörter erhalten ihre Einträge im Dateikatalog eine doppelte Qualität: neben der herkömmlichen Funktion, als Referenzinformation für von außen eingegebene Kennwörter zu dienen, sind sie nun selbst "Ausweise", die gegen die Referenzinformation in der Programm-Identifikations-Liste geprüft werden.

Mit einer Analyse verbleibender Probleme und Vorschlägen zu ihrer Bewältigung schließt die Arbeit.

6. SCHRIFTTUMSVERZEICHNIS

- [1] Ames, S.; J. K. Millen:
Interface Verification for a Security Kernel
Infotech State of Art Report - System Reliability and
Integrity (Vol. 2 - Invited Papers) 1978 pp. 1-21
- [2] Barber, B.; F. Gremy; K. Überla; G. Wagner [ed.]:
Medical Informatics Berlin 1979, Proceedings
Springer, Berlin/Heidelberg/New York 1979
- [3] Bates, W. S.:
Security of Computer-Based Information Systems
Datamation 16 (May 1970) pp. 41-64
- [4] Berson, T. A.; G. L. Barksdale Jr.:
KSOS - Development Methodology for a Secure Operating
System
Proc. AFIPs NCC 48 (June 1979) pp. 365-371
- [5] vor der Brück, H.:
Die grundlegenden Eigenschaften sicherer DV-Systeme
in Gliss, Hentschel [20]
- [6] Control Data Corporation:
NOS Version 1 Reference Manual
Publication Nr. 60435 400
- [7] Conway, R. W.; W. L. Maxwell; H. L. Morgan:
On the Implementation of Security Measures in
Information Systems
Comm. ACM 15 (Apr 1972) pp. 211-220
- [8] Denning, D. E.:
A Lattice Model of Secure Information Flow
Comm. ACM 19 (May 1976) pp. 236-243
- [9] Denning, D. E.; P. J. Denning:
Certification of Programs for a Secure Information
Flow
Comm. ACM 20 (July 1977) pp. 504-512
- [10] Denning, D. E.; P. J. Denning; M. D. Schwartz:
The Tracker: A Threat to Statistical Database Security
ACM Trans. on Database Systems 4 (Mar 1979) pp. 76-79
- [11] Dennis, J. B.; E. C. Van Horn:
Programming Semantics for Multiprogrammed Computations
Comm. ACM 9 (Mar 1966) pp. 143-155

- [12] Digital Equipment:
VAX - Technical Summary
Digital Equipment Corporation
- [13] Dijkstra, E. W.:
GO TO Statement Considered Harmful
Comm. ACM 11 (May 1968) letter to the editor p. 147
- [14] Dijkstra, E. W.:
Notes on Structured Programming
in
Dahl, O.-J.; E. W. Dijkstra; C. A. R. Hoare:
Structured Programming
Accademic Press, London/New York 1972
- [15] Dijkstra, E. W.:
The Humble Programmer
Comm. ACM 15 (Oct 1972) pp. 859-866
- [16] Dobkin, D.; A. K. Jones; R. J. Lipton:
Secure Databases: Protection against User Influence
ACM Trans. on Database Systems 4 (Mar 1979) pp. 97-106
- [17] Evans Jr., A.; W. Kantrowitz:
A User Authentication Scheme Not Requiring Secrecy in
the Computer
Comm. ACM 17 (Aug 1974) pp. 437-442
- [18] Fabry, R. S.:
Capability-Based Addressing
Comm. ACM 17 (July 1974) pp. 403-411
- [19] Gallwas, H.-U.; J. Schneider; J. Schweinoch;
T. Steinbrink:
Datenschutzrecht, Kommentar und Vorschriftensammlung
W. Kohlhammer, Stuttgart/Berlin/Köln/München 1979
- [20] Gliss, H.; B. Hentschel [ed.]
Bereichsspezifischer Datenschutz, technischer Daten-
schutz
Referate und Ergebnisse der 4. DAFTA
DATAKONTEXT-Verlag, Köln 1981
- [21] Gold, B. D.; R. R. Linde; R. J. Peeler; M. Schaefer;
J. F. Scheid; P. D. Ward:
A Security Retrofit of VM/370
Proc. AFIPs NCC 48 (June 1979) pp- 335-344
- [22] Graham, G. S.; P. J. Denning:
Protection - Principles and Practice
Proc. AFIPs SJCC 1972 pp. 417-429

- [23] Greiller, R.; K. Überla:
Data Security and Data Safety in Distributed Systems
Exemplified by the Medical Data Processing System
Munich
in
Lindberg, D. A. B.; S. Kaihara [ed.]:
Proc. of Third World Conf. on Medical Informatics
(MEDINFO)
North Holland, Amsterdam/New York/Oxford 1980
- [24] Greiser, E.:
Probleme des Datenbedarfs und Datenzugangs für die
epidemiologische Forschung
in Kilian, Porth [36]
- [25] Griese, J.; M. B. Plesch:
Datenschutzeinrichtungen in Datenbanksystemen
in
Nagel, K. [ed.]:
DV-Aktuell 1976
Science Research Associates (SRA), Stuttgart 1975
- [26] Griesser, G. [ed.]:
Realization of Data Protection in Health Information
Systems
Proc. of the IFIP-WG 4.2 Working Conference
North Holland, Amsterdam/New York/Oxford 1976
- [27] Griesser, G.:
Scope and Purpose
in Griesser [26]
- [28] Griesser, G.; A. Bakker; J. Danielsson; J.-C. Hirel;
D. J. Kenny; W. Schneider; A. I. Wassermann [ed.]:
Data Protection in Health Information Systems
North Holland, Amsterdam/New York/Oxford 1980
- [29] Harrison, M. A.; W. L. Ruzzo:
Protection in Operating Systems
Comm. ACM 19 (Aug 1976) pp. 461-471
- [30] Hoare, C. A. R.:
Monitors: An Operating System Structuring Concept
Comm. ACM 17 (Oct 1974) pp. 549-557
- [31] Hoffman, L. J.:
Modern Methods for Computer Security and Privacy
Prentice Hall, Englewood Cliffs, N.J. 1977

- [32] Hoffman, L. J.:
Computers and Privacy: A Survey
Comp. Surv. 1 (June 1969) pp. 85-103
- [33] Infotech:
Structured Programming
Infotech State of Art Report 1976
- [34] Kassel, H.; P. Strnad:
Lexikon Datenschutz und Datensicherung
Siemens-AG., Berlin/München 1978
- [35] Kilian, W.; K. Lenk; W. Steinmüller [ed.]
Datenschutz
S. Toeche-Mittler, Darmstadt 1973
- [36] Kilian, W.; A. J. Porth [ed.]
Juristische Probleme der Datenverarbeitung in der
Medizin
Springer, Berlin/Heidelberg/New York 1979
- [37] Klar, R.; P. Pietrzyk:
Datenschutzprobleme in einem Krankenhaus-Informationssystem
in Barber et al. [2]
- [38] Knuth, D. E.;
The Art of Computer Programming
Vol. 2, Seminumerical Algorithms
Addison-Wesley, Reading, Mass. 1969
- [39] Kriener; Michels:
Programmberechtigungstechnik - Kurzinformation
Mitteilung des Deutschen Instituts für medizinische
Dokumentation und Information (DIMDI)
- [40] Lampson, B. W.:
Dynamic Protection Structures
Proc. AFIPs FJCC 1969 pp. 27-38
- [41] Lampson, B. W.:
A Note on the Confinement Problem
Comm. ACM 16 (Oct 1973) pp. 613-615
- [42] Lenk, K.:
Datenschutz in der öffentlichen Verwaltung
in Kilian et al. [35]

- [43] Lindemann, P.; K. Nagel; G. Herrmann:
Organisation des Datenschutzes
Luchterhand, Neuwied/Berlin 1973
- [44] Linden T. A.:
Operating System Structures to Support Security and
Reliable Software
Comp. Surv. 8 (Dec 1976) pp. 409-445
- [45] Mallmann, C.:
Datenschutz in Verwaltungsinformations-Systemen
Oldenbourg, München/Wien 1976
- [46] Martin, J.:
Security, Accuracy and Privacy in Computer Systems
Prentice Hall, Englewood Cliffs, N.J. 1973
- [47] McCauley, E. J.; P. J. Drangowski:
KSOS - The Description of a Secure Operating System
Proc. AFIPs NCC 48 (June 1979) pp. 345-353
- [48] Millen, J. K.:
Security Kernel Validation in Practice
Comm. ACM 19 (May 1976) pp. 243-250
- [49] Palme, J.:
Software Security
Datamation 20 (Jan 1974) pp. 51-55
- [50] Petersen, H.; B.-I. Niemi-Johansson; A. M. Lind;
O. Mellon; K. Thurfors:
Improvement of a Security System
in Barber et al. [2]
- [51] Petersen, H. E.; R. Turn:
System Applications of Information Privacy
Proc. AFIPs SJCC 1976 pp. 291-299
- [52] Popek, G. J.; C. S. Kline:
A Verifiable Protection System
Proc. Intern. Conf. on Reliable Software
ACM SIGPLAN Notices 10 (June 1975) pp. 294-304
- [53] Popek, G. J.; D. A. Farber:
A Model for Verification of Data Security in Operating
Systems
Comm. ACM 21 (Sept. 1978) pp. 737-749

- [54] Popek, G. J. & M. Karpstein: *Security & Confidentiality*
M. Urbaniak, E. J. McLaughlin
UCLA Security Unit
Proc. AFIPS NCS 44 (June 1973) pp. 333-340
- [55] Purdy, G. B.:
A High Security LDC-IN Structure
Comm. ACM 17 Aug 1974 pp. 442-443
- [56] Reichertz, P. L.:
Realization of Data Protection in Software Structures
in Grieser [26]
- [57] Reichertz, P. L. & W. Kilian (Ed.):
Arztgenehmnis - Datenbanken - Datenschutz
Springer, Berlin/Heidelberg 1974
- [58] Reichertz, P. L.:
Kontextabhängigkeit medizinischer Informationssysteme
in Reichertz, Kilian [57]
- [59] Rienhoff, O.:
Die Darstellung der Datenstruktur in der Medizin
Daten in der medizinischen Dokumentation
in Reichertz, Kilian [57]
- [60] Rüdell, W.:
Darstellung und Vergleich verschiedener Modelle zur
Beschreibung geschützter Systeme
Arbeitsberichte des Inst. f. Med. Wissenschaften zur
Datenverarbeitung, Universität Erlanger Nürnberg
Band 10, Nr. 9, 1977
- [61] Saltzer, J. H.:
Protection and the Control of Information Flowing in
MULTICS
Comm. ACM 17 (July 1974) pp. 388-402
- [62] Saltzer, J. H.; M. D. Schroeder:
The Protection of Information in Computer Systems
Proc. IEEE 63 (Sept 1975) pp. 1278-1308
- [63] Schlörner, J.:
Statistical Database Security: Some Recent Results
in Barber et al. [2]
- [64] Schneider, J.:
Technische Möglichkeiten des Datenschutzes
in Kilian et al. [39]

- [65] Schroeder, M. D.; J. H. Saltzer:
A Hardware Architecture for Implementing Protection Rings
Comm. ACM 15 (Mar 1972) pp. 157-170
- [66] Schulze, J. H.:
Datenschutz in der Datenverarbeitung
IBM-Nachrichten 205 (Feb 1971) pp. 640-645
- [67] Sieber, U.:
Urheberrechtliche und wettbewerbsrechtliche Erfassung
der unbefugten Softwarenutzung
in Gliss, Hentschel [20]
- [68] Siemens:
Kommandosprache des Organisationsprogramms BS2000
Beschreibung
Siemens-AG., Best.-Nr. D15/5136-08
- [69] Sperry Univac:
Series 1100 Executive System Level 37R1 Security System
Sperry Corporation, UP-Number 8934
- [70] Sperry Univac:
DPS 1100 User Reference
Sperry Corporation, UP-Number 8992
- [71] Stadler, N.:
Datensicherung durch Organisation
Rudolf Haufe Verlag, Freiburg i.Br. 1980
- [72] Steinmüller, W.:
Objektbereich "Verwaltungsinformation" und Prinzipien
des Datenschutzes
in Kilian et al. [35]
- [73] Steinmüller, W.; L. Ermer; W. Schimmel:
Datenschutz bei riskanten Systemen
Springer, Berlin/Heidelberg/New York 1978
- [74] Sterling, Th. D.:
Guidelines for Humanising Information Systems
A Report from Stanley House
Comm. ACM 17 (Nov 1974) pp. 609-613
- [75] Stout, R.:
Wer kennt Ritchie Blake?
Fernsehspiel aus der Serie "Nero Wolfe", gesendet vom
österreichischen Rundfunk, 1. Programm am 14.4.1983

- [76] Turn, R.; W. H. Ware:
Privacy and Security in Computer Systems
American Scientist 63 (Mar 1975) pp. 196-203
- [77] Überla, K.; J. Zeiler [ed.]:
Datenschutz und Wissenschaftsadministration im
Gesundheitsbereich
BGA-Schriften 5/83
MMV Medizin Verlag München 1983
- [78] Wagner, G.:
Krebsregister und Datenschutz
in Kilian, Porth [36]
- [79] Walter, K. G.; S. I. Shaen; W. F. Ogden; W. C. Rounds;
D. G. Shumway; D. D. Schaeffer; K. J. Biba;
F. T. Bradshaw; S. R. Ames; J. M. Gilligan:
Structured Specification of a Security Kernel
Proc. Intern. Conf. on Reliable Software
ACM SIGPLAN Notices 10 (June 1975) pp. 285-293
- [80] Wood, H. M.:
On-Line Password Techniques
Symposium Proc. Trends and Applications 1977
Computer Security and Integrity (May 1977) pp. 27-31
- [81] Wulf, W.; M. Shaw:
Global Variable Considered Harmful
ACM SIGPLAN Notices 8 (Feb 1973) pp. 28-34
- [82] Wulf, W.; E. Cohen; W. Corwin; A. Jones; R. Levin;
C. Pierson; F. Pollak:
HYDRA: The Kernel of a Multiprocessor Operating System
Comm. ACM 17 (June 1974) pp. 337-345
- [83] Young, C. R.:
A Security Policy for a Profile Oriented Operating
System
Proc. AFIPs NCC 50 (1981) pp. 273-282
- [84] Zeiler, J.:
Datenschutz im Bundesgesundheitsamt
in Überla, Zeiler 77
- [85] -:
Monatsspektrum: Konflikt um Krebsregister und
Datenschutz
Spektrum der Wissenschaft (Juni 1983) pp. 16-17

L E B E N S L A U F

Name	Bernd Alexander Wilhelm Albertus M e y e r - B e n d e r
Geburtsdatum	16. Dezember 1934
Geburtsort	Bonn/Rh.
Eltern	Dr. jur. Karl E. Meyer und Frau Gertrud M. Meyer

Schulausbildung

4.41 - 7.47	Schüler am Vorschul-Internat "St. John's Preparatory School", Alton Castle, Alton, N. Staffs. England
9.47 - 7.51	Schüler am Internat "Cotton College" Cotton, N. Staffs. England
7.51	"General Certificate of Education, Ordinary Level" des zentralen Prü- fungsausschusses der Universitäten Oxford und Cambridge (entspricht in etwa der Mittleren Reife)
9.51 - 3.52	Gastschüler am Gymnasium an der Kreuzgasse, Köln
4.52 - 3.55	Schüler am Goethe-Gymnasium, Karlsruhe
10.3.55	Reifeprüfung

Hochschulausbildung

1.4.55 - 30.9.55	Hochschulpraktikant, Fa. Siemens & Halske, Karlsruhe
WS 55/56 - WS 57/58	Studium, Fachrichtung Elektrotechnik TH Karlsruhe
WS 56/57 und SS 57	Diplom-Vorprüfung Gesamturteil "Sehr gut bestanden"
SS 58 - WS 61/62	Studium, Fachrichtung Elektrotechnik TH München
3.59 - 5.59	Fachpraktikum am Institut für el. Nachrichtentechnik und Meßtechnik, TH München
SS 59 und WS 59/60	Einzelprüfungen der Diplom-Hauptprü- fung, Gesamturteil "Sehr gut bestanden"
WS 59/60 - WS 61/62	Diplomarbeit "Entwurf und Aufbau eines Praktikumsmodells: Dynamische Schalt- kreistechnik", Bewertung "Mit Aus- zeichnung"
SS 60 und WS 60/61	Gasthörer an der LMU
SS 62 - WS 63/64	Studium, Fachrichtung Mathematik, LMU
Ostern 1964	Abbruch des Zweitstudiums wegen Vermählung

Beruflicher Werdegang

1.5.63 - 31.3.66	Institut für Nachrichtentechnik TH München
1.5.63 - 30.9.64	Wissenschaftliche Hilfskraft
1.10.64 - 31.3.66	Wissenschaftlicher Mitarbeiter
1.4.66 - 30.9.70	Institut für Datenverarbeitung TH München
1.4.66 - 31.8.67	Wissenschaftliche Hilfskraft mit der Funktion und den Bezügen eines Wissenschaftlichen Assistenten
1.9.67 - 30.9.70	Wissenschaftlicher Assistent
ab SS 67	Schriftführer des Diplom-Haupt- prüfungsausschusses für Elektro- technik
seit 1.10.70	Stellvertretender Leiter des Rechen- zentrums der LMU für die Medizinische Fakultät (zunächst EDV-Abteilung des Klinikums Großhadern)
1.10.70 - 30.11.70	Wissenschaftlicher Assistent
1.12.70 - 31.7.72	Akademischer Rat
1.8.72 - 10.4.80	Akademischer Oberrat
seit 11.4.80	Akademischer Direktor

